

Mediant™ 800 MSBR

Multi-Service Business Router

Session Border Controller

# User's Manual



Version 6.6

December 2013

Document # LTRT-12811





---

## Table of Contents

---

<b>1</b>	<b>Overview .....</b>	<b>19</b>
<hr/>		
<b>Part I - Getting Started with Initial Connectivity.....</b>		<b>21</b>
<b>2</b>	<b>Introduction .....</b>	<b>23</b>
<b>3</b>	<b>Configuring VoIP-LAN Interface for OAMP .....</b>	<b>25</b>
3.1	Web Interface .....	25
3.2	CLI .....	27
<b>4</b>	<b>Configuring Data-Router's LAN and WAN .....</b>	<b>29</b>
4.1	Configuring Data-Router's LAN Interface.....	29
4.2	Configuring the Device's DHCP Server .....	30
4.3	Configuring the WAN Interface .....	30
<b>5</b>	<b>Enabling Remote Management from WAN.....</b>	<b>33</b>
5.1	Remote Web-based (HTTP/S) Management .....	33
5.2	Remote Telnet-based Management .....	34
<hr/>		
<b>Part II - Management Tools .....</b>		<b>35</b>
<b>6</b>	<b>Introduction .....</b>	<b>37</b>
<b>7</b>	<b>Web-Based Management.....</b>	<b>39</b>
7.1	Getting Acquainted with the Web Interface .....	39
7.1.1	Computer Requirements.....	39
7.1.2	Accessing the Web Interface .....	40
7.1.3	Areas of the GUI .....	40
7.1.4	Toolbar Description.....	41
7.1.5	Navigation Tree .....	42
7.1.5.1	Displaying Navigation Tree in Basic and Full View .....	43
7.1.5.2	Showing / Hiding the Navigation Pane.....	44
7.1.6	Working with Configuration Pages .....	45
7.1.6.1	Accessing Pages.....	45
7.1.6.2	Viewing Parameters .....	45
7.1.6.3	Modifying and Saving Parameters .....	47
7.1.6.4	Working with Tables .....	48
7.1.7	Searching for Configuration Parameters .....	50
7.1.8	Creating a Login Welcome Message.....	52
7.1.9	Getting Help .....	53
7.1.10	Logging Off the Web Interface.....	54
7.2	Viewing the Home Page .....	54
7.2.1	Assigning a Port Name .....	57
7.3	Configuring Web User Accounts.....	58
7.3.1	Basic User Accounts Configuration .....	59
7.3.2	Advanced User Accounts Configuration.....	61
7.4	Displaying Login Information upon Login .....	64
7.5	Configuring Web Security Settings .....	65
7.6	Limiting OAMP Access to a Specific WAN Interface .....	66

7.7	Web Login Authentication using Smart Cards.....	66
7.8	Configuring Web and Telnet Access List .....	67
7.9	Configuring RADIUS Settings.....	68
<b>8</b>	<b>CLI-Based Management.....</b>	<b>69</b>
8.1	Enabling CLI using Telnet.....	69
8.2	Enabling CLI using SSH and RSA Public Key .....	70
8.3	Establishing a CLI Session .....	72
8.4	Configuring TACACS+ for CLI Login .....	73
<b>9</b>	<b>SNMP-Based Management .....</b>	<b>75</b>
9.1	Configuring SNMP Community Strings .....	75
9.2	Configuring SNMP Trap Destinations .....	76
9.3	Configuring SNMP Trusted Managers .....	77
9.4	Configuring SNMP V3 Users .....	78
<b>10</b>	<b>EMS-Based Management.....</b>	<b>81</b>
<b>11</b>	<b>TR-069 CWMP Based Management .....</b>	<b>83</b>
11.1	TR-069 .....	83
11.2	TR-104 .....	86
11.3	Configuring TR-069 .....	88
<b>12</b>	<b>INI File-Based Management.....</b>	<b>89</b>
12.1	INI File Format.....	89
12.1.1	Configuring Individual ini File Parameters .....	89
12.1.2	Configuring Table ini File Parameters .....	89
12.1.3	General ini File Formatting Rules .....	91
12.2	Loading an ini File .....	91
12.3	Modifying an ini File.....	92
12.4	Secured Encoded ini File.....	92
<b>Part III - General System Settings .....</b>		<b>93</b>
<b>13</b>	<b>Configuring Certificates .....</b>	<b>95</b>
13.1	Replacing the Device's Certificate .....	95
13.2	Loading a Private Key .....	96
13.3	Mutual TLS Authentication.....	98
13.4	Self-Signed Certificates .....	98
13.5	Configuring Certificate Revocation Checking (OCSP) .....	99
13.6	TLS Server Certificate Expiry Check .....	99
13.7	Loading Certificate Chain for Trusted Root.....	100
<b>14</b>	<b>Date and Time.....</b>	<b>101</b>
14.1	Configuring Date and Time Manually.....	101
14.2	Automatic Date and Time through SNTP Server .....	101
<b>15</b>	<b>Configuring Power over Ethernet .....</b>	<b>103</b>
<b>Part IV - General VoIP Configuration .....</b>		<b>105</b>



<b>16 Network</b>	<b>107</b>
16.1 Configuring IP Network Interfaces	107
16.1.1 Assigning NTP Services to Application Types	111
16.1.2 Multiple Interface Table Configuration Rules	111
16.1.3 Troubleshooting the Multiple Interface Table	112
16.1.4 Networking Configuration Examples	112
16.1.4.1 One VoIP Interface for All Applications	112
16.1.4.2 VoIP Interface per Application Type	113
16.1.4.3 VoIP Interfaces for Combined Application Types	113
16.1.4.4 VoIP Interfaces with Multiple Default Gateways	114
16.2 Configuring the IP Routing Table	115
16.2.1 Interface Column	117
16.2.2 Routing Table Configuration Summary and Guidelines	117
16.2.3 Troubleshooting the Routing Table	117
16.3 Configuring Quality of Service	118
16.4 DNS	120
16.4.1 Configuring the Internal DNS Table	120
16.4.2 Configuring the Internal SRV Table	121
16.5 Configuring NFS Settings	123
16.6 Network Address Translation Support	125
16.6.1 Device Located behind NAT	125
16.6.1.1 Configuring a Static NAT IP Address for All Interfaces	126
16.6.1.2 Configuring NAT Translation per IP Interface	127
16.6.2 Remote UA behind NAT	128
16.6.2.1 First Incoming Packet Mechanism	129
16.6.2.2 No-Op Packets	129
16.7 Robust Receipt of Media Streams	130
16.8 Multiple Routers Support	130
<b>17 Security</b>	<b>131</b>
17.1 Configuring Firewall Settings	131
17.2 Configuring General Security Settings	135
17.3 Intrusion Detection System	136
17.3.1 Enabling IDS	136
17.3.2 Configuring IDS Policies	137
17.3.3 Assigning IDS Policies	140
17.3.4 Viewing IDS Alarms	142
<b>18 Media</b>	<b>145</b>
18.1 Configuring Voice Settings	145
18.1.1 Configuring Voice Gain (Volume) Control	145
18.1.2 Silence Suppression (Compression)	146
18.1.3 Echo Cancellation	146
18.2 Fax and Modem Capabilities	148
18.2.1 Fax/Modem Operating Modes	149
18.2.2 Fax/Modem Transport Modes	149
18.2.2.1 T.38 Fax Relay Mode	149
18.2.2.2 G.711 Fax / Modem Transport Mode	151
18.2.2.3 Fax Fallback	151
18.2.2.4 Fax/Modem Bypass Mode	152
18.2.2.5 Fax / Modem NSE Mode	153
18.2.2.6 Fax / Modem Transparent with Events Mode	154
18.2.2.7 Fax / Modem Transparent Mode	154

18.2.2.8	RFC 2833 ANS Report upon Fax/Modem Detection .....	155
18.2.3	V.34 Fax Support.....	155
18.2.3.1	Bypass Mechanism for V.34 Fax Transmission .....	156
18.2.3.2	Relay Mode for T.30 and V.34 Faxes .....	156
18.2.3.3	V.34 Fax Relay for SG3 Fax Machines.....	157
18.2.4	V.150.1 Modem Relay .....	158
18.2.5	Simultaneous Negotiation of Fax (T.38) and Modem (V.150.1) Relay.....	159
18.2.6	V.152 Support.....	160
18.2.7	Fax Transmission behind NAT .....	161
18.3	Configuring RTP/RTCP Settings.....	161
18.3.1	Configuring the Dynamic Jitter Buffer.....	161
18.3.2	Comfort Noise Generation .....	162
18.3.3	Dual-Tone Multi-Frequency Signaling .....	163
18.3.3.1	Configuring DTMF Transport Types.....	163
18.3.3.2	Configuring RFC 2833 Payload .....	164
18.3.4	Configuring RTP Base UDP Port.....	165
18.4	Configuring IP Media Settings .....	166
18.4.1	Automatic Gain Control (AGC) .....	166
18.5	Configuring Analog Settings .....	167
18.6	Configuring Various Codec Attributes.....	167
18.7	Configuring Media Realms .....	168
18.7.1	Configuring Quality of Experience per Media Realm .....	170
18.7.2	Configuring Bandwidth Management per Media Realm.....	173
18.8	Configuring Server for Media Quality of Experience .....	175
18.9	Configuring Media Security.....	176
<b>19</b>	<b>Services .....</b>	<b>179</b>
19.1	Routing Based on LDAP Active Directory Queries.....	179
19.1.1	Configuring the LDAP Server .....	179
19.1.2	Configuring the Device's LDAP Cache.....	180
19.1.3	Active Directory based Tel-to-IP Routing for Microsoft Lync.....	182
19.1.3.1	Querying the AD and Routing Priority .....	182
19.1.3.2	Configuring AD-Based Routing Rules.....	185
19.1.3.3	Querying the AD for Calling Name.....	188
19.2	Least Cost Routing.....	189
19.2.1	Overview .....	189
19.2.2	Configuring LCR .....	191
19.2.2.1	Enabling the LCR Feature.....	191
19.2.2.2	Configuring Cost Groups.....	193
19.2.2.3	Configuring Time Bands for Cost Groups .....	194
19.2.2.4	Assigning Cost Groups to Routing Rules.....	196
<b>20</b>	<b>Enabling Applications.....</b>	<b>197</b>
<b>21</b>	<b>Control Network .....</b>	<b>199</b>
21.1	Configuring SRD Table.....	199
21.2	Configuring SIP Interface Table.....	201
21.3	Configuring IP Groups .....	204
21.4	Configuring Proxy Sets Table .....	213
21.5	Associating WAN Interface with VoIP Traffic .....	217
<b>22</b>	<b>SIP Definitions.....</b>	<b>219</b>
22.1	Configuring SIP Parameters .....	219
22.2	Configuring Account Table .....	219

22.3	Configuring Proxy and Registration Parameters .....	222
22.3.1	SIP Message Authentication Example .....	224
22.4	Configuring SIP Message Manipulation .....	226
22.5	Configuring SIP Message Policy Rules.....	230
<b>23</b>	<b>Coders and Profiles .....</b>	<b>233</b>
23.1	Configuring Coders.....	233
23.2	Configuring Coders Groups.....	236
23.3	Configuring Tel Profile .....	237
23.4	Configuring IP Profiles.....	239
<b>Part V - Gateway and IP-to-IP Application .....</b>		<b>251</b>
<b>24</b>	<b>IP-to-IP Routing Overview .....</b>	<b>253</b>
24.1	Theory of Operation.....	254
24.1.1	Proxy Sets .....	255
24.1.2	IP Groups.....	255
24.1.3	Inbound and Outbound IP Routing Rules.....	257
24.1.4	Accounts .....	257
24.2	IP-to-IP Routing Configuration Example .....	257
24.2.1	Step 1: Enable the IP-to-IP Capabilities .....	260
24.2.2	Step 2: Configure the Number of Media Channels.....	260
24.2.3	Step 3: Define a Trunk Group for the Local PSTN .....	260
24.2.4	Step 4: Configure the Proxy Sets .....	261
24.2.5	Step 5: Configure the IP Groups .....	263
24.2.6	Step 6: Configure the Account Table.....	264
24.2.7	Step 7: Configure IP Profiles for Voice Coders .....	265
24.2.8	Step 8: Configure Inbound IP Routing.....	266
24.2.9	Step 9: Configure Outbound IP Routing.....	268
24.2.10	Step 10: Configure Destination Phone Number Manipulation.....	269
<b>25</b>	<b>Digital PSTN.....</b>	<b>271</b>
25.1	Configuring Trunk Settings .....	271
25.2	TDM and Timing.....	274
25.2.1	Configuring TDM Bus Settings .....	274
25.2.2	Clock Settings.....	274
25.2.2.1	Recovering Clock from PSTN Line Interface .....	275
25.2.2.2	Configuring Internal Clock as Clock Source.....	275
25.3	Configuring CAS State Machines .....	276
25.4	Configuring Digital Gateway Parameters .....	278
25.5	Tunneling Applications .....	279
25.5.1	TDM Tunneling .....	279
25.5.1.1	DSP Pattern Detector.....	282
25.5.2	QSIG Tunneling .....	282
25.6	ISDN Non-Facility Associated Signaling (NFAS) .....	283
25.6.1	NFAS Interface ID.....	284
25.6.2	Working with DMS-100 Switches .....	284
25.6.3	Creating an NFAS-Related Trunk Configuration .....	285
25.6.4	Performing Manual D-Channel Switchover in NFAS Group.....	286
25.7	ISDN Overlap Dialing .....	286
25.7.1	Collecting ISDN Digits and Sending Complete Number in SIP .....	286
25.7.2	Interworking ISDN Overlap Dialing with SIP According to RFC 3578.....	287

25.8 Redirect Number and Calling Name (Display) .....	288
<b>26 Trunk Group .....</b>	<b>289</b>
26.1 Configuring Trunk Group Table .....	289
26.2 Configuring Hunt Group Settings .....	291
<b>27 Manipulation .....</b>	<b>297</b>
27.1 Configuring General Settings.....	297
27.2 Configuring Source/Destination Number Manipulation Rules.....	297
27.3 Manipulating Number Prefix .....	303
27.4 SIP Calling Name Manipulations .....	304
27.5 Configuring Redirect Number IP to Tel .....	307
27.6 Manipulating Redirected and Diverted Numbers for Call Diversion .....	310
27.7 Mapping NPI/TON to SIP Phone-Context .....	311
27.8 Configuring Release Cause Mapping .....	313
27.8.1 Fixed Mapping of SIP Response to ISDN Release Reason.....	314
27.8.2 Fixed Mapping of ISDN Release Reason to SIP Response.....	316
27.8.3 Reason Header.....	318
27.8.4 Mapping PSTN Release Cause to SIP Response .....	318
27.9 Numbering Plans and Type of Number .....	319
<b>28 Routing.....</b>	<b>321</b>
28.1 Configuring General Routing Parameters .....	321
28.2 Configuring Outbound IP Routing Table .....	321
28.3 Configuring Inbound IP Routing Table .....	330
28.4 IP Destinations Connectivity Feature .....	334
28.5 Alternative Routing for Tel-to-IP Calls.....	335
28.5.1 Alternative Routing Based on IP Connectivity .....	335
28.5.2 Alternative Routing Based on SIP Responses .....	336
28.5.3 PSTN Fallback.....	338
28.6 Alternative Routing for IP-to-Tel Calls.....	339
28.6.1 Alternative Routing to Trunk upon Q.931 Call Release Cause Code .....	339
28.6.2 Alternative Routing to an IP Destination upon a Busy Trunk .....	340
<b>29 Configuring DTMF and Dialing.....</b>	<b>343</b>
29.1 Dialing Plan Features .....	344
29.1.1 Digit Mapping.....	344
29.1.2 External Dial Plan File .....	345
<b>30 Configuring Supplementary Services .....</b>	<b>347</b>
30.1 Call Hold and Retrieve.....	349
30.2 Call Pickup .....	351
30.3 BRI Suspend and Resume .....	351
30.4 Consultation Feature .....	352
30.5 Call Transfer.....	352
30.5.1 Consultation Call Transfer .....	352
30.5.2 Consultation Transfer for QSIG Path Replacement .....	353
30.5.3 Blind Call Transfer .....	353
30.6 Call Forward .....	354
30.6.1 Call Forward Reminder Ring .....	355
30.6.2 Call Forward Reminder (Off-Hook) Special Dial Tone .....	355
30.6.3 Call Forward Reminder Dial Tone (Off-Hook) upon Spanish SIP Alert-Info.....	356

30.6.4 BRI Call Forwarding.....	357
30.7 Call Waiting .....	357
30.8 Message Waiting Indication.....	358
30.9 Caller ID .....	360
30.9.1 Caller ID Detection / Generation on the Tel Side .....	360
30.9.2 Debugging a Caller ID Detection on FXO.....	360
30.9.3 Caller ID on the IP Side .....	361
30.10 Three-Way Conferencing.....	362
30.11 Emergency E911 Phone Number Services.....	363
30.11.1 FXS Device Emulating PSAP using DID Loop-Start Lines.....	364
30.11.2 FXO Device Interworking SIP E911 Calls from Service Provider's IP Network to PSAP DID Lines .....	366
30.11.3 Pre-empting Existing Calls for E911 IP-to-Tel Calls .....	369
30.11.4 Enhanced 9-1-1 Support for Lync Server 2010.....	370
30.11.4.1 About E9-1-1 Services .....	370
30.11.4.2 Microsoft Lync Server 2010 and E9-1-1.....	371
30.11.4.3 AudioCodes ELIN Gateway for Lync Server 2010 E9-1-1 Calls to PSTN 375	
30.11.4.4 Configuring AudioCodes ELIN Gateway .....	380
30.12 Multilevel Precedence and Preemption.....	382
30.12.1 MLPP Preemption Events in SIP Reason Header .....	384
30.12.2 Precedence Ring Tone .....	385
30.13 Denial of Collect Calls .....	385
30.14 Configuring ISDN Supplementary Services .....	386
30.15 Advice of Charge Services for Euro ISDN .....	388
30.16 Configuring Voice Mail.....	389
<b>31 Analog Gateway .....</b>	<b>391</b>
31.1 Configuring Keypad Features .....	391
31.2 Configuring Metering Tones .....	392
31.3 Configuring Charge Codes .....	393
31.4 Configuring FXO Settings.....	394
31.5 Configuring Authentication.....	395
31.6 Configuring Automatic Dialing .....	396
31.7 Configuring Caller Display Information.....	398
31.8 Configuring Call Forward.....	399
31.9 Configuring Caller ID Permissions.....	401
31.10 Configuring Call Waiting .....	402
31.11 Rejecting Anonymous Calls.....	403
31.12 Configuring FXS Distinctive Ringing and Call Waiting Tones per Source/Destination Number.....	403
31.13 FXS/FXO Coefficient Types.....	405
31.14 FXO Operating Modes.....	405
31.14.1 FXO Operations for IP-to-Tel Calls.....	406
31.14.1.1 One-Stage Dialing .....	406
31.14.1.2 Two-Stage Dialing .....	407
31.14.1.3 DID Wink .....	407
31.14.2 FXO Operations for Tel-to-IP Calls.....	408
31.14.2.1 Automatic Dialing .....	408
31.14.2.2 Collecting Digits Mode.....	409
31.14.2.3 FXO Supplementary Services.....	409

31.14.3 Call Termination on FXO Devices .....	410
31.14.3.1 Calls Termination by PBX .....	410
31.14.3.2 Call Termination before Call Establishment .....	411
31.14.3.3 Ring Detection Timeout .....	411
31.15 Remote PBX Extension between FXO and FXS Devices .....	411
31.15.1 Dialing from Remote Extension (Phone at FXS) .....	412
31.15.2 Dialing from PBX Line or PSTN .....	412
31.15.3 Message Waiting Indication for Remote Extensions .....	413
31.15.4 Call Waiting for Remote Extensions .....	413
31.15.5 FXS Gateway Configuration .....	414
31.15.6 FXO Gateway Configuration .....	415

## **Part VI - Session Border Controller Application .....417**

### **32 SBC Overview .....419**

32.1 SIP Network Definitions .....	420
32.2 SIP Dialog Initiation Process .....	420
32.3 User Registration and Internal Database .....	422
32.3.1 Initial Registration Request Processing .....	423
32.3.2 Internal Database .....	423
32.3.3 Routing using Internal Database .....	424
32.3.4 Registration Refreshes .....	424
32.3.5 Notification of Expired User Registration to SIP Proxy / Registrar .....	424
32.3.6 Registration Restriction Control .....	425
32.4 SBC Media Handling .....	425
32.4.1 Media Anchoring without Transcoding (Transparent) .....	427
32.4.2 Media Anchoring with Transcoding .....	427
32.4.3 No Media Anchoring .....	429
32.4.4 Transcoding Modes .....	431
32.4.5 Restricting Coders .....	431
32.4.6 Coder Transcoding .....	432
32.4.7 Prioritizing Coder List in SDP Offer .....	433
32.4.8 SRTP-RTP and SRTP-SRTP Transcoding .....	433
32.4.9 Multiple RTP Media Streams per Call Session .....	434
32.4.10 Interworking DTMF Methods .....	434
32.5 Fax Negotiation and Transcoding .....	435
32.6 Limiting SBC Call Duration .....	435
32.7 SIP Authentication Server for SBC Users .....	435
32.8 Interworking SIP Signaling .....	436
32.8.1 Interworking SIP 3xx Redirect Responses .....	436
32.8.1.1 Resultant INVITE Traversing Device .....	436
32.8.1.2 Local Handling of SIP 3xx .....	438
32.8.2 Interworking SIP Diversion and History-Info Headers .....	438
32.8.3 Interworking SIP REFER Messages .....	439
32.8.4 Interworking SIP PRACK Messages .....	439
32.8.5 Interworking SIP Session Timer .....	440
32.8.6 Interworking SIP Early Media .....	440
32.8.7 Interworking SIP re-INVITE Messages .....	442
32.8.8 Interworking SIP UPDATE Messages .....	442
32.8.9 Interworking SIP re-INVITE to UPDATE .....	442
32.8.10 Interworking Delayed Offer .....	442
32.8.11 Interworking Call Hold .....	443
32.9 Call Survivability .....	443
32.9.1 Auto-Provisioning of Subscriber-Specific Information for BroadWorks Server for Survivability .....	443

32.9.2	BroadSoft's Shared Phone Line Call Appearance for SBC Survivability.....	444
32.9.3	Call Survivability for Call Centers .....	445
32.9.4	Survivability Mode Display on Aastra IP Phones .....	447
32.10	Call Forking .....	448
32.10.1	Initiating SIP Call Forking .....	448
32.10.2	SIP Forking Initiated by SIP Proxy Server.....	448
32.11	Alternative Routing on Detection of Failed SIP Response .....	449
<b>33</b>	<b>SBC Configuration .....</b>	<b>451</b>
33.1	Configuring General Settings.....	451
33.2	Configuring Admission Control .....	452
33.3	Configuring Allowed Coder Groups .....	454
33.4	Routing SBC.....	455
33.4.1	Configuring Classification Rules.....	456
33.4.1.1	Classification Based on URI of Selected Header Example.....	460
33.4.2	Configuring Condition Rules.....	461
33.4.3	Configuring SBC IP-to-IP Routing .....	462
33.4.4	Configuring Alternative Routing Reasons.....	468
33.5	SBC Manipulations .....	469
33.5.1	Configuring IP-to-IP Inbound Manipulations.....	471
33.5.2	Configuring IP-to-IP Outbound Manipulations.....	474
<b>Part VII - Cloud Resilience Package Application .....</b>		<b>479</b>
<b>34</b>	<b>CRP Overview .....</b>	<b>481</b>
<b>35</b>	<b>CRP Configuration .....</b>	<b>483</b>
35.1	Enabling the CRP Application.....	483
35.2	Configuring Call Survivability Mode .....	484
35.3	Pre-Configured IP Groups .....	485
35.4	Pre-Configured IP-to-IP Routing Rules .....	486
<b>Part VIII - Stand-Alone Survivability Application .....</b>		<b>487</b>
<b>36</b>	<b>SAS Overview .....</b>	<b>489</b>
36.1	SAS Operating Modes.....	489
36.1.1	SAS Outbound Mode.....	490
36.1.1.1	Normal State .....	490
36.1.1.2	Emergency State.....	490
36.1.2	SAS Redundant Mode.....	491
36.1.2.1	Normal State .....	492
36.1.2.2	Emergency State.....	492
36.1.2.3	Exiting Emergency and Returning to Normal State .....	492
36.2	SAS Routing.....	493
36.2.1	SAS Routing in Normal State .....	493
36.2.2	SAS Routing in Emergency State.....	495
<b>37</b>	<b>SAS Configuration .....</b>	<b>497</b>
37.1	General SAS Configuration .....	497
37.1.1	Enabling the SAS Application.....	497
37.1.2	Configuring Common SAS Parameters.....	497

37.2	Configuring SAS Outbound Mode.....	500
37.3	Configuring SAS Redundant Mode.....	500
37.4	Configuring Gateway Application with SAS .....	501
37.4.1	Gateway with SAS Outbound Mode .....	501
37.4.2	Gateway with SAS Redundant Mode .....	502
37.5	Advanced SAS Configuration .....	504
37.5.1	Manipulating URI user part of Incoming REGISTER.....	504
37.5.2	Manipulating Destination Number of Incoming INVITE .....	505
37.5.3	SAS Routing Based on IP-to-IP Routing Table .....	508
37.5.4	Blocking Calls from Unregistered SAS Users.....	513
37.5.5	Configuring SAS Emergency Calls .....	513
37.5.6	Adding SIP Record-Route Header to SIP INVITE .....	514
37.5.7	Re-using TCP Connections .....	514
37.5.8	Replacing Contact Header for SIP Messages .....	515
37.6	Viewing Registered SAS Users .....	516
<b>38</b>	<b>SAS Cascading.....</b>	<b>517</b>
<b>Part IX - IP Media Capabilities .....</b>		<b>519</b>
<b>39</b>	<b>Transcoding using Third-Party Call Control .....</b>	<b>521</b>
39.1	Using RFC 4117 .....	521
<b>Part X - Data-Router Configuration .....</b>		<b>523</b>
<b>40</b>	<b>Introduction .....</b>	<b>525</b>
<b>Part XI - Maintenance .....</b>		<b>527</b>
<b>41</b>	<b>Basic Maintenance .....</b>	<b>529</b>
41.1	Resetting the Device .....	529
41.2	Remotely Resetting Device using SIP NOTIFY .....	530
41.3	Locking and Unlocking the Device .....	531
41.4	Saving Configuration .....	532
<b>42</b>	<b>Resetting Channels.....</b>	<b>533</b>
42.1	Resetting an Analog Channel .....	533
42.2	Restarting a B-Channel .....	533
<b>43</b>	<b>Software Upgrade.....</b>	<b>535</b>
43.1	Loading Auxiliary Files.....	535
43.1.1	Call Progress Tones File .....	537
43.1.1.1	Distinctive Ringing.....	539
43.1.2	CAS Files .....	541
43.1.3	Dial Plan File.....	541
43.1.3.1	Creating a Dial Plan File.....	541
43.1.3.2	Dialing Plans for Digit Collection .....	542
43.1.3.3	Dial Plan Prefix Tags for IP-to-Tel Routing .....	544
43.1.3.4	Obtaining IP Destination from Dial Plan File .....	546
43.1.3.5	Modifying ISDN-to-IP Calling Party Number .....	546
43.1.4	User Information File .....	547
43.1.4.1	User Information File for PBX Extensions and "Global" Numbers .....	548



43.1.4.2	User Information File for SBC User Database .....	549
43.1.4.3	Configuring User Info Table using CLI .....	550
43.1.4.4	Enabling the User Info Table.....	551
43.2	Software License Key .....	552
43.2.1	Obtaining the Software License Key File.....	552
43.2.2	Installing the Software License Key.....	553
43.2.2.1	Installing the Software License Key using Web .....	553
43.2.2.2	Installing the Software License Key using CLI .....	554
43.3	Software Upgrade Wizard.....	555
43.4	Backing Up and Loading Configuration File .....	558
<b>44</b>	<b>Automatic Update.....</b>	<b>561</b>
44.1	Configuring Automatic Update .....	562
44.2	Obtaining IP Address Automatically using DHCP .....	564
44.3	Automatic Configuration Methods.....	565
44.3.1	DHCP-based Configuration Server .....	565
44.3.2	HTTP-based Automatic Updates.....	565
44.3.3	Configuration using FTP or NFS .....	566
44.3.4	Configuration using AudioCodes EMS .....	566
44.4	Loading Files Securely by Disabling TFTP .....	566
44.5	Remotely Triggering Auto Update using SIP NOTIFY.....	567
44.6	Configuring Zero Configuration.....	568
<b>45</b>	<b>Restoring Factory Defaults .....</b>	<b>571</b>
45.1	Restoring Defaults using CLI .....	571
45.2	Restoring Defaults using Hardware Reset Button.....	572
45.3	Restoring Defaults using an ini File .....	572
<b>46</b>	<b>USB Storage Capabilities .....</b>	<b>573</b>
<b>Part XII - Status, Performance Monitoring and Reporting.....</b>		<b>575</b>
<b>47</b>	<b>System Status .....</b>	<b>577</b>
47.1	Viewing Device Information .....	577
47.2	Viewing Ethernet Port Information .....	577
<b>48</b>	<b>Carrier-Grade Alarms.....</b>	<b>579</b>
48.1	Viewing Active Alarms .....	579
48.2	Viewing Alarm History .....	579
<b>49</b>	<b>Performance Monitoring.....</b>	<b>581</b>
49.1	Viewing MOS per Media Realm.....	581
49.2	Viewing Trunk Utilization .....	582
49.3	Viewing Quality of Experience .....	583
49.4	Viewing Average Call Duration .....	584
49.5	Network Monitoring (Probing) Two Devices .....	585
<b>50</b>	<b>VoIP Status .....</b>	<b>589</b>
50.1	Viewing Trunks & Channels Status.....	589
50.2	Viewing Analog Port Information.....	590

50.3	Viewing NFAS Groups and D-Channel Status .....	591
50.4	Viewing Active IP Interfaces .....	592
50.5	Viewing Performance Statistics .....	592
50.6	Viewing Call Counters .....	592
50.7	Viewing Registered Users .....	594
50.8	Viewing Registration Status.....	595
50.9	Viewing Call Routing Status .....	596
50.10	Viewing IP Connectivity .....	597
<b>51</b>	<b>Data Status .....</b>	<b>599</b>
51.1	Viewing WAN Status .....	599
51.2	Viewing Network Connection Statistics.....	600
51.3	Viewing Logged Security Events .....	601
51.4	Viewing QoS Queues Statistics .....	603
51.5	Viewing Logged Data Events.....	603
<b>52</b>	<b>Reporting Information to External Party .....</b>	<b>605</b>
52.1	RTP Control Protocol Extended Reports (RTCP XR).....	605
52.2	Generating Call Detail Records .....	608
52.2.1	Configuring CDR Reporting .....	608
52.2.2	CDR Field Description .....	609
52.2.2.1	CDR Fields for SBC Signaling .....	609
52.2.2.2	CDR Fields for SBC Media.....	611
52.2.2.3	CDR Fields for Gateway/IP-to-IP Application.....	612
52.2.2.4	Release Reasons in CDR .....	616
52.3	Configuring RADIUS Accounting .....	619
52.4	Querying Device Channel Resources using SIP OPTIONS .....	622
<b>Part XIII - Diagnostics.....</b>		<b>623</b>
<b>53</b>	<b>Syslog and Debug Recordings .....</b>	<b>625</b>
53.1	Syslog Message Format.....	625
53.1.1	Event Representation in Syslog Messages .....	626
53.1.2	Unique Device Identification in Syslog Messages .....	628
53.1.3	Identifying AudioCodes Syslog Messages using Facility Levels .....	628
53.1.4	SNMP Alarms in Syslog Messages .....	629
53.2	Configuring Syslog Settings.....	629
53.3	Configuring Debug Recording .....	630
53.4	Filtering Syslog Messages and Debug Recordings.....	631
53.4.1	Filtering IP Network Traces .....	633
53.5	Viewing Syslog Messages .....	634
53.6	Collecting Debug Recording Messages .....	636
53.7	Capturing VoIP and Data-Router Network Traffic .....	638
<b>54</b>	<b>Self-Testing.....</b>	<b>639</b>
<b>55</b>	<b>Analog Line Testing.....</b>	<b>641</b>
<b>56</b>	<b>Testing SIP Signaling Calls .....</b>	<b>643</b>
56.1	Configuring Test Call Endpoints .....	643
56.1.1	Starting, Stopping and Restarting Test Calls.....	646

56.1.2 Viewing Test Call Statistics.....	647
56.2 Configuring DTMF Tones for Test Calls.....	648
56.3 Configuring Basic Test Call .....	649
56.4 Configuring SBC Test Call with External Proxy.....	650
56.5 Test Call Configuration Examples.....	651
<b>57 Running Data-Router Diagnostic Tests.....</b>	<b>655</b>
<b>Part XIV - Appendix .....</b>	<b>657</b>
<b>58 Dialing Plan Notation for Routing and Manipulation.....</b>	<b>659</b>
<b>59 Configuration Parameters Reference .....</b>	<b>661</b>
59.1 Networking Parameters .....	661
59.1.1 Multiple VoIP Network Interfaces and VLAN Parameters .....	661
59.1.2 Routing Parameters.....	662
59.1.3 Quality of Service Parameters.....	662
59.1.4 NAT and STUN Parameters .....	663
59.1.5 NFS Parameters .....	664
59.1.6 DNS Parameters.....	665
59.1.7 DHCP Parameters .....	665
59.1.8 NTP and Daylight Saving Time Parameters.....	666
59.1.9 Power over Ethernet Parameters .....	667
59.2 Management Parameters .....	668
59.2.1 General Parameters .....	668
59.2.2 Web Parameters.....	669
59.2.3 Telnet Parameters .....	671
59.2.4 SNMP Parameters.....	672
59.2.5 CLI Parameters.....	675
59.2.6 TR-069 Parameters .....	675
59.2.7 Serial Parameters .....	677
59.3 Debugging and Diagnostics Parameters.....	678
59.3.1 General Parameters .....	678
59.3.2 SIP Test Call Parameters .....	679
59.3.3 Syslog, CDR and Debug Parameters.....	680
59.3.4 Resource Allocation Indication Parameters.....	684
59.4 Security Parameters .....	685
59.4.1 General Parameters .....	685
59.4.2 HTTPS Parameters .....	686
59.4.3 SRTP Parameters.....	687
59.4.4 TLS Parameters.....	690
59.4.5 SSH Parameters.....	692
59.4.6 OCSP Parameters .....	693
59.4.7 IDS Parameters .....	694
59.5 RADIUS Parameters .....	695
59.6 SIP Media Realm Parameters .....	697
59.7 Control Network Parameters .....	699
59.7.1 IP Group, Proxy, Registration and Authentication Parameters .....	699
59.7.2 Network Application Parameters .....	710
59.8 General SIP Parameters .....	712
59.9 Coders and Profile Parameters.....	740
59.10 Channel Parameters.....	744
59.10.1 Voice Parameters .....	744

59.10.2	Coder Parameters .....	747
59.10.3	DTMF Parameters .....	748
59.10.4	RTP, RTCP and T.38 Parameters .....	749
59.11	Gateway and IP-to-IP Parameters .....	753
59.11.1	Fax and Modem Parameters .....	753
59.11.2	DTMF and Hook-Flash Parameters .....	760
59.11.3	Digit Collection and Dial Plan Parameters .....	765
59.11.4	Voice Mail Parameters .....	767
59.11.5	Supplementary Services Parameters .....	773
59.11.5.1	Caller ID Parameters .....	773
59.11.5.2	Call Waiting Parameters .....	777
59.11.5.3	Call Forwarding Parameters .....	779
59.11.5.4	Message Waiting Indication Parameters .....	781
59.11.5.5	Call Hold Parameters .....	783
59.11.5.6	Call Transfer Parameters .....	784
59.11.5.7	Three-Way Conferencing Parameters .....	787
59.11.5.8	MLPP and Emergency Call Parameters .....	788
59.11.5.9	Call Cut-Through Parameters .....	794
59.11.5.10	Automatic Dialing Parameters .....	795
59.11.5.11	Direct Inward Dialing Parameters .....	795
59.11.5.12	ISDN BRI Parameters .....	797
59.11.6	PSTN Parameters .....	799
59.11.6.1	General Parameters .....	799
59.11.6.2	TDM Bus and Clock Timing Parameters .....	803
59.11.6.3	CAS Parameters .....	805
59.11.6.4	ISDN Parameters .....	808
59.11.7	ISDN and CAS Interworking Parameters .....	815
59.11.8	Answer and Disconnect Supervision Parameters .....	830
59.11.9	Tone Parameters .....	834
59.11.9.1	Telephony Tone Parameters .....	834
59.11.9.2	Tone Detection Parameters .....	841
59.11.9.3	Metering Tone Parameters .....	843
59.11.10	Telephone Keypad Sequence Parameters .....	844
59.11.11	General FXO Parameters .....	847
59.11.12	Trunk Groups and Routing Parameters .....	850
59.11.13	IP Connectivity Parameters .....	856
59.11.14	Alternative Routing Parameters .....	857
59.11.15	Number Manipulation Parameters .....	859
59.12	Least Cost Routing Parameters .....	869
59.13	LDAP Parameters .....	870
59.14	SBC and CRP Parameters .....	873
59.15	Standalone Survivability Parameters .....	885
59.16	IP Media Parameters .....	889
59.17	Auxiliary and Configuration File Name Parameters .....	893
59.18	Automatic Update Parameters .....	894
<b>60</b>	<b>DSP Templates .....</b>	<b>897</b>
<b>61</b>	<b>Technical Specifications .....</b>	<b>899</b>

## Notice

This document describes the AudioCodes Mediant 800 Multi-Service Business Router (MSBR).

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 2013 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: December-12-2013

## Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI<sup>2</sup>, CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

## WEEE EU Directive

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

## Customer Support

Customer technical support and service are generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact [support@audiocodes.com](mailto:support@audiocodes.com).

## Abbreviations and Terminology

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

Throughout this manual, unless otherwise specified, the term *device* refers to the Mediant 800 MSBR.

## Related Documentation

Manual Name
SIP CPE Release Notes
Mediant 800 MSBR Hardware Installation Manual
MSBR Series CLI Reference Guide for Data Functionality
MSBR Series CLI Reference Guide for VoIP and System Functionality
SBC Design Guide
DConvert User's Guide
CPTWizard User's Guide



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



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



**Note:** This device is considered an **INDOOR** unit and therefore must be installed only indoors.



**Note:** The device's installed Software License Key does not include the MSFT feature key, which enables the device to operate in a Microsoft Lync Server environment. If necessary, you can order this feature key separately from your AudioCodes sales representative.



**Notes:**

- 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](mailto:eay@cryptsoft.com)).

# 1 Overview

The Mediant 800 Multi-Service Business Router (MSBR) is a networking device that combines multiple service functions such as a Media Gateway, Session Border Controller (SBC), Data Router and Firewall, LAN switch, WAN access, Stand Alone Survivability (SAS) and an integrated general-purpose server. The device offers enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications, as well as flexible PSTN and legacy PBX connectivity.

The device is designed as a secured Voice-over-IP (VoIP) and data platform. Enhanced media gateway security features include, for example, SRTP for media, TLS for SIP control, and IPSec for management. Data security functions include integrated Stateful Firewall, IDS/IPS, SSL for remote user access, and site-to-site VPN. A fully featured enterprise class SBC provides a secured voice network deployment based on a Back-to-Back User Agent (B2BUA) implementation.

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

The device provides Foreign Exchange Station (FXS) and/or Foreign Exchange Office (FXO) telephony module interfaces, depending on ordered hardware configuration. The device supports either a combination of FXS and FXO port interfaces, or only FXS or only FXO interfaces. The device can support up to 12 simultaneous VoIP calls. Each FXS or FXO module provides four analog RJ-11 ports. The FXO module can be used to connect analog lines of an enterprise's PBX or the PSTN, to the IP network. The FXS module can be used to connect legacy telephones, fax machines, and modems to the IP network. Optionally, the FXS module can be connected to the external trunk lines of a PBX. When deployed with a combination of FXO and FXS modules, the device can be used as a PBX for Small Office Home Office (SOHO) users, and businesses not equipped with a PBX. The FXS modules also support the Analog Lifeline feature, enabling an FXS port to connect directly to the PSTN upon power and/or network failure.

The device supports up to 8 ISDN Basic Rate Interface (BRI) S/T interfaces (RJ-45 ports), supporting up to 16 voice channels. These connect ISDN terminal equipment such as ISDN telephones. The device also provides an optional, single E1/T1 interface port, supporting Transparent, CAS and ISDN protocols. The device supports various ISDN PRI protocols such as Euro ISDN, North American NI2, Lucent™ 4/5ESS, Nortel™ DMS-100 and others. It also supports various ISDN BRI protocols such as ETSI 5ESS and QSIG over BRI. It also supports different variants of CAS protocols for E1 and T1 spans, including MFC R2, E&M immediate start, E&M delay dial / start, loop start and ground start.

The device's data routing capabilities support static and dynamic routing protocols such as RIP/OSPF and BGP, Virtual Routing and Forwarding (VRF-Lite) where interfaces can be clustered into a VRF to provide segregated routing domains. The device supports various optional WAN interfaces, providing flexibility in connecting to Service Providers:

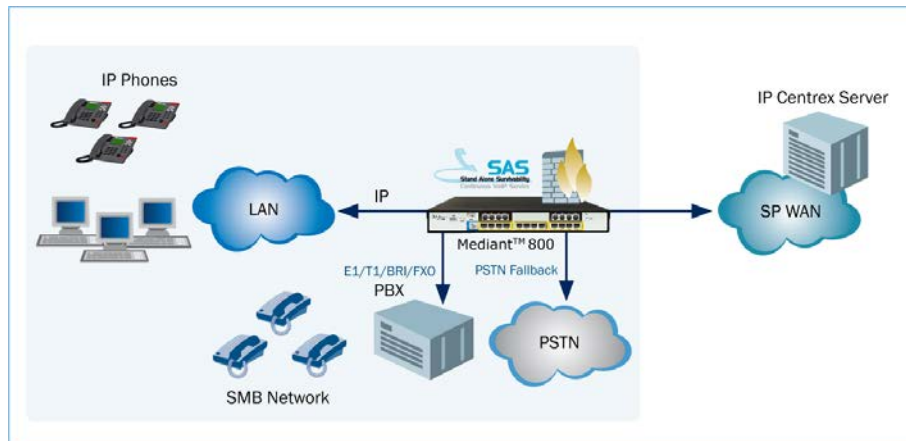
- 1000Base-T Gigabit Ethernet copper.
- Symmetric High-Speed Digital Subscriber Line (SHDSL) - supports up to four copper wire pairs according to G.991.2, acting as a remote-terminal CPE device. Both ATM and EFM modes are supported. In the ATM mode, a variety of protocols are supported, including PPPoE, PPPoA, and RFC 2684 in both bridged (Ethernet-over-ATM) and routed (IP-over-ATM) variants. In the EFM mode, the SHDSL port functions as a logical Ethernet device.
- ADSL/VDSL
- 3G Cellular modem using a USB connection - this can be used as the primary WAN interface or as a WAN backup in case of failure in the WAN connection (provided by any of the above).



The device is optimized for wire-speed delivery of data, providing up to 12 Ethernet LAN ports for connecting equipment such as computers and IP phones. These ports are divided into Gigabit Ethernet and Fast Ethernet interfaces (the number depends on the ordered configuration), and provide power-over-Ethernet (PoE) capabilities. The device also supports an optional, Wi-Fi interface, providing wireless LAN 802.11n access point at 2.4 GHz, 3Tx/3Rx enabling data rates of up to 300 Mbps. The Wi-Fi interface also supports 802.11b/802.11g backward compatibility, allowing interoperability of multiple devices with different types of Wi-Fi

The device also provides an integrated Open Solution Network (OSN) Server module. The OSN can host a variety of third-party applications such as IP-PBX, Call Center, and Conferencing.

**Figure 1-1: Typical Application**



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



**Note:** You can configure the Data-Routing functionality **only** through CLI. However, AudioCodes recommends that you also use CLI to configure all other device configuration (VoIP and System). For information on configuring the device through CLI, refer to the following documents:

- **Data-Router functionality:** *MSBR Series CLI Reference Guide for Data Functionality*
- **System and VoIP functionality:** *MSBR Series CLI Reference Guide for System and VoIP Functionalities*



# Part I

## Getting Started with Initial Connectivity



## 2 Introduction

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

The device is shipped with a factory default IP address for operations, administration, maintenance, and provisioning (OAMP) through the VoIP LAN interface. You can use this address to initially access the device using any of its management tools -- embedded Web server, EMS, or Telnet.

You can also access the device through the console CLI, whereby the device's serial (RS-232) port is connected to the management PC's serial port.

Device management can be done through one of the VoIP LAN OAMP, WAN, and LAN.



**Note:** By default, the device's embedded DHCP server is enabled. For more information, see Section 'Configuring the Device's DHCP Server' on page [30](#).

## Reader's Notes

## 3 Configuring VoIP-LAN Interface for OAMP

You can configure the VoIP LAN OAMP through the device's Web interface or CLI.

### 3.1 Web Interface

This procedure describes how to configure the VoIP-LAN IP address for OAMP, through the Web interface.

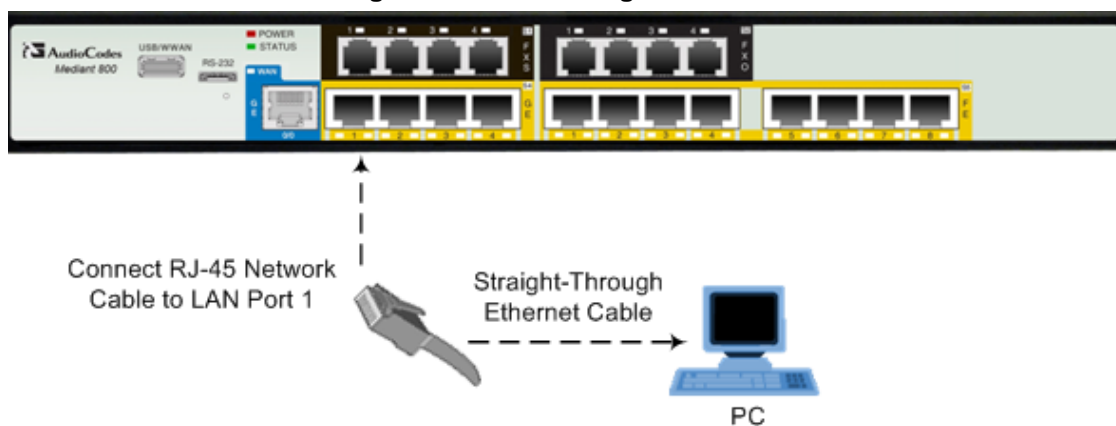
**Default VoIP LAN IP Address for OAMP**

IP Address	Value
IP Address	192.168.0.2
Subnet Mask	255.255.255.0
Default Gateway IP Address	192.168.0.1

➤ **To configure the VoIP-LAN IP address for OAMP:**

1. Connect Port 1 (left-most LAN port), located on the front panel, directly to the network interface of your computer, using a straight-through Ethernet cable.

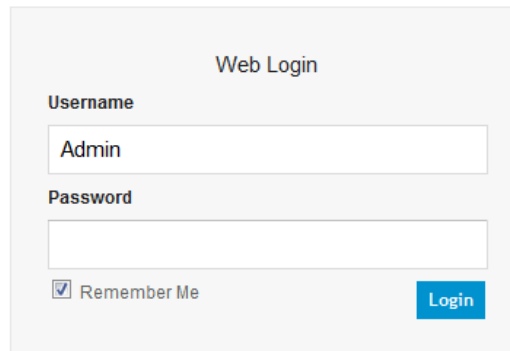
**Figure 3-1: Connecting to LAN Port**



2. Make sure that your computer is configured to automatically obtain an IP address; the device has an embedded DHCP server which by default allocates IP addresses to computers that are connected to it.

3. On your computer, start a Web browser and in the URL address field, enter the default IP address of the device; the Web interface's Web Login screen appears:

**Figure 3-2: Web Login Screen**



Web Login

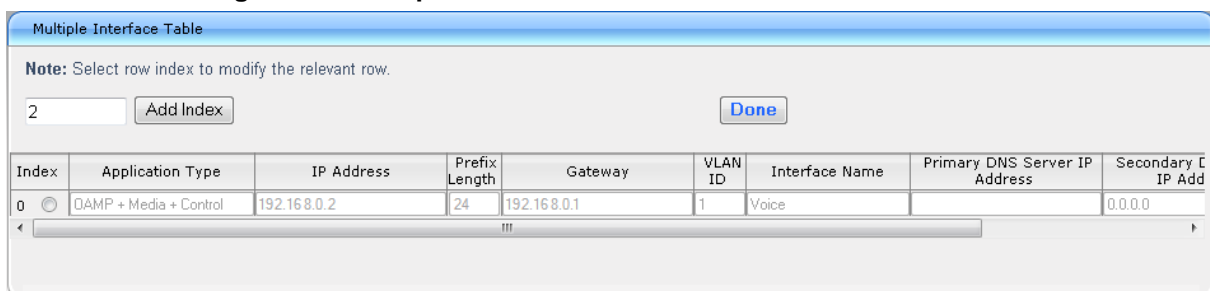
Username  
Admin

Password

☒ Remember Me Login

4. In the 'Username' and 'Password' fields, enter the default (case-sensitive) login username ("Admin") and password ("Admin"), and then click **Login**; the device's Web interface appears.
5. Open the Multiple Interface Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**).

**Figure 3-3: Multiple Interface Table with Default OAMP Address**



**Note:** Select row index to modify the relevant row.

2 Add Index Done

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address
0	OAMP + Media + Control	192.168.0.2	24	192.168.0.1	1	Voice		0.0.0.0

- a. Select the 'Index' radio button corresponding to the "OAMP + Media + Control" application type, and then click **Edit**.
  - b. Change the IP address to correspond with your network IP addressing scheme, for example:
    - ◆ IP Address: 10.8.6.86
    - ◆ Prefix Length: 24 (for 255.255.255.0)
    - ◆ Gateway: 10.8.6.85
  - c. Click **Apply**, and then click **Done** to validate your settings.
6. Reset the device with a flash burn.
  7. Cable the device to your network. You can now access the management interface using the new IP address for OAMP.



**Note:** when you complete the above procedure, change your PC's IP address to correspond with your network requirements.

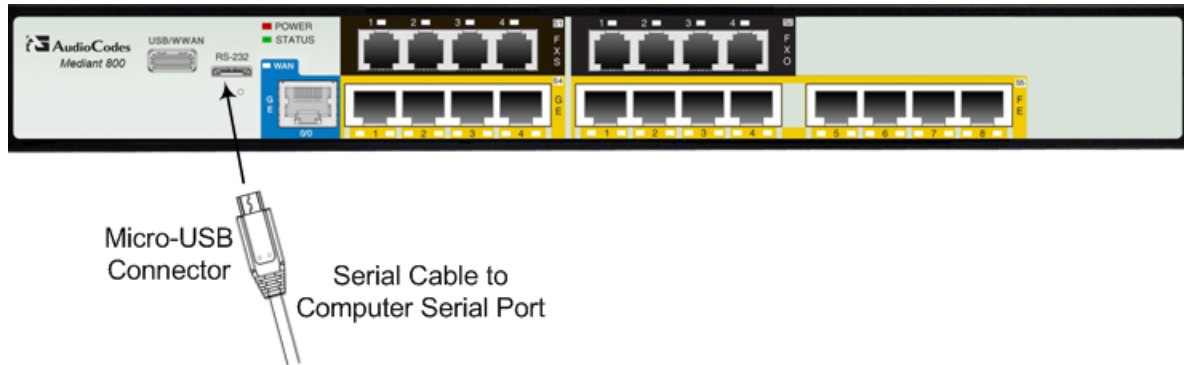
## 3.2 CLI

This procedure describes how to configure the VoIP-LAN IP address for OAMP, through the CLI.

➤ **To configure the VoIP-LAN IP address for OAMP:**

1. Connect the RS-232 port of the device to the serial communication port on your computer. For more information, refer to the *Hardware Installation Manual*.

**Figure 3-4: Connecting to Serial Port**



2. Establish serial communication with the device using a terminal emulator 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
3. At the CLI prompt, type the username (default is "Admin" - case sensitive):  
Username: Admin
4. At the prompt, type the password (default is "Admin" - case sensitive):  
Password: Admin
5. At the prompt, type the following:  
**enable**
6. At the prompt, type the password again:  
Password: Admin
7. Access the VoIP configuration mode:  
**# configure voip**
8. Access the Multiple Interface table:  
(config-voip)# **interface network-if 0**
9. Configure the IP address:  
(network-if-0)# **set ip** <IP address>
10. Configure the prefix length:  
(network-if-0)# **set prefix-length** <prefix length, e.g., 16>
11. Configure the Default Gateway address:  
(network-if-0)# **set gateway** <IP address>

12. Exit the Multiple Interface table:  
`(network-if-0)# exit`
13. Exit the VoIP configuration mode:  
`(config-voip)# exit`
14. Reset the device with a flash burn:  
`# reload now`
15. Cable the device to your network. You can now access the management interface using the new IP address for OAMP.



**Note:** After you have completed the above procedure, change your PC's IP address according to your network requirements.



## 4 Configuring Data-Router's LAN and WAN

This section describes how to configure the device's data-router LAN and/or WAN interfaces.



### Notes:

- Make sure that you configure the LAN IP address of the data-router in the **same** subnet as the LAN IP address for OAMP of the VoIP interface.
- Once you access the device through the default VoIP LAN interface, you can configure Web management access from one of the following interfaces:
  - ✓ Any of the configured data-router LAN interfaces. The default LAN data interface is 192.168.0.1. This interface can be in a different subnet to the VoIP LAN IP address and with a different VLAN ID. This is useful, for example, if you want to separate management from the VoIP traffic.
  - ✓ WAN port interface. In this setup, you need to enable remote access to the WAN port interface, as described in 'Enabling Remote Management from WAN' on page 32.

### 4.1 Configuring Data-Router's LAN Interface

The default LAN IP address of the device's data-router is listed in the table below.

**Default LAN IP Address of Data-Router**

Parameter	Default Value
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0

#### ➤ To configure LAN IP address of data-router:

1. Establish serial communication with the device.
2. At the prompt, type the following command to access the data-router configuration mode:

```
# configure data
```

3. Access the VLAN 1 LAN switch interface:

```
(config-data)# interface vlan 1
```

4. Configure the IP address and subnet:

```
(conf-if-VLAN 1)# ip address <IP address> <subnet>
```

For example:

```
(conf-if-VLAN 1)# ip address 10.8.6.85 255.255.255.0
```

5. Save your settings with a flash burn:

```
(conf-if-VLAN 1)# do write
```

## 4.2 Configuring the Device's DHCP Server

By default, the device's embedded DHCP server is enabled for the LAN, and with default IP pool addresses relating to the default subnet LAN. You can disable the DHCP server, or modify the IP address pool. The device's DHCP server allocates this spool of IP addresses to the computers connected to its LAN interface.

➤ **To enable the device's DHCP server:**

1. Establish serial communication with the device.
2. At the prompt, type the following command to access the Data-router configuration mode:

```
# configure data
```

3. Access the data LAN switch interface:

```
(config-data)# interface vlan 1
```

4. To disable the DHCP server:

```
(conf-if-VLAN 1)# no service dhcp
```

5. To enable DHCP server:

- a. Configure the pool of IP addresses:

```
(conf-if-VLAN 1)# ip dhcp-server network 10.8.6.84 10.8.6.89  
255.255.255.0
```

- b. Enable DHCP server functionality:

```
(conf-if-VLAN 1)# service dhcp
```

6. Save your settings with a flash burn:

```
(conf-if-VLAN 1)# do write
```

## 4.3 Configuring the WAN Interface

This procedure describes how to configure the WAN interface and uses Gigabit Ethernet as an example. If your device uses a different WAN interface, refer to the *MSBR Series CLI Reference Guide for Data*.



**Note:** Before you configure the WAN interface, make sure that you have all the required information from your Internet Telephony Service Provider (ITSP).

➤ **To configure a WAN IP address:**

1. Connect the WAN port to the WAN network. For information on cabling the WAN port, refer to the *Hardware Installation Manual*.
2. Establish serial communication with the device.
3. At the prompt, type the following command to access the Data-router configuration mode:

```
# configure data
```

4. Access the WAN interface:

```
(config-data)# interface GigabitEthernet 0/0
```

5. Configure the IP address and subnet mask:

```
(config-if-GE 0/0)# ip address 100.33.2.105 255.255.255.0
```

6. Enable Network Address Port Translation (NAPT) on the WAN interface:

```
(config-if-GE 0/0)# napt
```

7. Enable the WAN interface:

```
(config-if-GE 0/0)# no shutdown
```

8. Exit the interface:

```
(config-if-GE 0/0)# exit
```

9. Configure the default route:

```
(config-data)# ip route 0.0.0.0 0.0.0.0 100.33.2.106  
GigabitEthernet 0/0
```

10. Exit the data-router configuration mode:

```
(config-data)# exit
```

11. Save the configuration to flash:

```
# write
```

## Reader's Notes

## 5 Enabling Remote Management from WAN

This section describes how to configure remote device management from the WAN, if necessary.

### 5.1 Remote Web-based (HTTP/S) Management

This procedure describes how to enable remote Web-based management (HTTP/S) from the WAN.

➤ **To enable remote Web (HTTP/S) management from WAN:**

■ **CLI:**

1. Access the System configuration mode:

```
# configure system
```

2. Enable HTTP management from the WAN:

```
<config-system># web
```

```
<web># set wan-http on
```

3. Reset the device with a burn to flash:

```
<cli-terminal># do reload now
```

■ **Web:**

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

**Figure 5-1: Enabling Web Management from WAN**

General	
Voice Menu Password	12345
HTTP Authentication Mode	Web Based Authentication
Secured Web Connection (HTTPS)	HTTP and HTTPS
Requires Client Certificates for HTTPS connection	Disable
HTTPS Cipher String	RC4:EXP
WAN OAMP Interface	WAN Ethernet
Allow WAN access to HTTP	Disable
Allow WAN access to HTTPS	Enable

2. From the 'WAN OAMP Interface' drop-down list, select the WAN interface (**WAN Ethernet**).
3. From the 'Allow WAN access to HTTPS' drop-down list, select **Enable**.
4. Click **Submit**.
5. Save your settings with a flash burn.

## 5.2 Remote Telnet-based Management

This procedure describes how to enable remote Telnet-based management from the WAN.

### ➤ To enable remote Telnet management from WAN:

#### ■ CLI:

1. Access the System configuration mode:

```
# configure system
```

2. Type the following command:

```
<config-system># cli-terminal
```

3. Enable Telnet:

```
<cli-terminal># set telnet
```

4. Enable Telnet from WAN:

```
<cli-terminal># set wan-telnet-allow on
```

5. Reset the device with a burn to flash:

```
<cli-terminal># do reload now
```

#### ■ Web:

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

**Figure 5-2: Enabling Telnet Management from WAN**

▼ Telnet Settings	
Embedded Telnet Server	Enable Secured ▼
Telnet Server TCP Port	23
⚡ Telnet Server Idle Timeout	100
⚡ Allow WAN access to Telnet	Enable ▼

2. From the 'Embedded Telnet Server' drop-down list, select **Enable Secured**.
3. From the 'Allow WAN access to Telnet' drop-down list, select **Enable**.
4. Click **Submit**.
5. Save your settings with a flash burn.

# Part II

## Management Tools





## 6 Introduction

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

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

- Embedded HTTP/S-based Web server - see 'Web-based Management' on page [39](#)
- Command Line Interface (CLI) - see 'CLI-Based Management' on page [69](#)
- AudioCodes Element Management System - see EMS-Based Management on page [81](#)
- Simple Network Management Protocol (SNMP) browser software - see 'SNMP-Based Management' on page [75](#)
- TR-069 - see TR-069 Based Management on page [83](#)
- Configuration *ini* file - see 'INI File-Based Management' on page [89](#)

**Notes:**

- Some configuration settings can only be done using a specific management tool. For example, some configuration can only be done using the Configuration ini file method.
- Throughout this manual, where a parameter is mentioned, its corresponding Web, CLI, and ini parameter is mentioned. The ini file parameters are enclosed in square brackets [...].
- For a list and description of all the configuration parameters, see 'Configuration Parameters Reference' on page [661](#).

## Reader's Notes

## 7 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, data routing, and various traffic parameters

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

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



**Notes:**

- The Web interface allows you to configure most of the device's settings. However, additional configuration parameters may exist that are not available in the Web interface and which can only be configured using other management tools.
- Some Web interface pages and/or parameters are available only for certain hardware configurations or software features. The software features are determined by the installed Software License Key (see 'Software License Key' on page 552).

### 7.1 Getting Acquainted with the Web Interface

This section provides a description of the Web interface.

#### 7.1.1 Computer Requirements

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

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



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

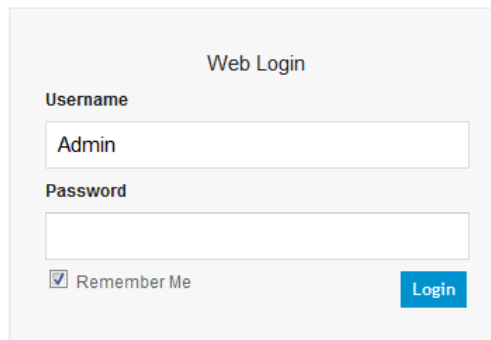
## 7.1.2 Accessing the Web Interface

The procedure below describes how to access the Web interface.

➤ **To access the Web interface:**

1. Open a standard Web browser (see 'Computer Requirements' on page 39).
2. In the Web browser, specify the IP address of the device (e.g., <http://10.1.10.10>); the Web interface's Login window appears, as shown below:

**Figure 7-1: Web Login Screen**



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

3. In the 'Username' and 'Password' fields, enter the case-sensitive, user name and password respectively.
4. Click **Login**; the Web interface is accessed, displaying the Home page. For a detailed description of the Home page, see 'Viewing the Home Page' on page 54.



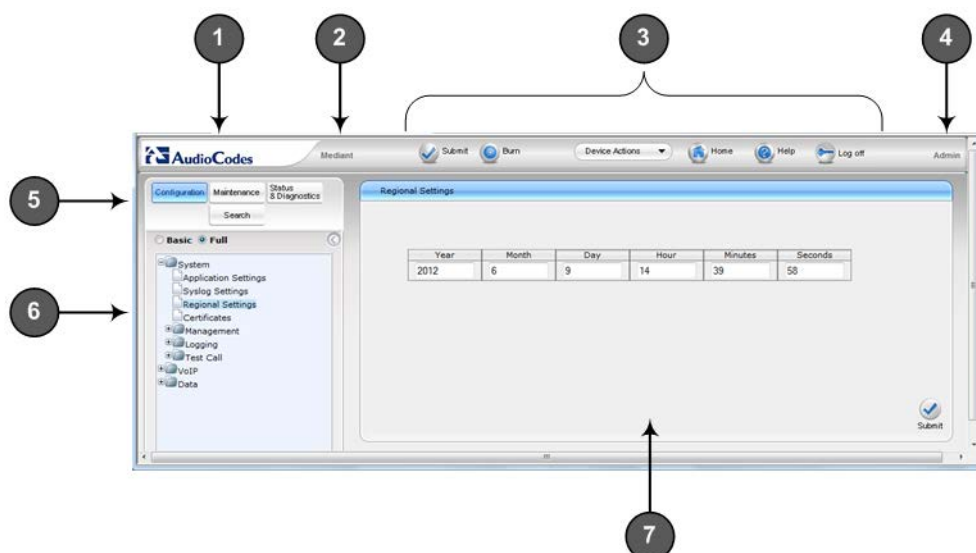
**Notes:**

- The default username and password is "Admin". To change the login user name and password, see 'Configuring the Web User Accounts' on page 58.
- If you want the Web browser to remember your password, select the 'Remember Me' check box and then agree to the browser's prompt (depending on your browser) to save the password for future logins. On your next login attempt, simply press the Tab or Enter keys to auto-fill the 'Username' and 'Password' fields, and then click **Login**.

## 7.1.3 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 7-2: Areas of Web GUI



Description of the Web GUI Areas


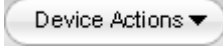



Item #	Description
1	Displays AudioCodes (corporate) logo image.
2	Displays the product name.
3	Toolbar, providing frequently required command buttons. For more information, see 'Toolbar Description' on page 41.
4	Displays the username of the Web user that is currently logged in.
5	Navigation bar, providing the following tabs for accessing various functionalities in the Navigation tree: <ul style="list-style-type: none"> <li>▪ <b>Configuration, Maintenance, and Status &amp; Diagnostics</b> tabs: Access the configuration menus (see 'Working with Configuration Pages' on page 45)</li> <li>▪ <b>Search</b> tab: Enables a search engine for searching configuration parameters (see 'Searching for Configuration Parameters' on page 50)</li> </ul>
6	Navigation tree, displaying a tree-like structure of elements (configuration menus or search engine) pertaining to the selected tab on the Navigation bar. For more information, see 'Navigation Tree' on page 42.
7	Work pane, displaying the configuration page of the selected menu in the Navigation tree. This is where configuration is done. For more information, see 'Working with Configuration Pages' on page 45.

### 7.1.4 Toolbar Description

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

Description of Toolbar Buttons

Icon	Button Name	Description
	<b>Submit</b>	Applies parameter settings to the device (see 'Saving Configuration' on page 532).

Icon	Button Name	Description
		<b>Note:</b> This icon is grayed out when not applicable to the currently opened page.
	<b>Burn</b>	Saves parameter settings to flash memory (see 'Saving Configuration' on page 532).
	<b>Device Actions</b>	Opens a drop-down list with frequently needed commands: <ul style="list-style-type: none"> <li>▪ <b>Load Configuration File:</b> Opens the Configuration File page for loading an <i>ini</i> file to the device (see 'Backing Up and Loading Configuration File' on page 558).</li> <li>▪ <b>Save Configuration File:</b> Opens the Configuration File page for saving the <i>ini</i> file to a folder on a computer (see 'Backing Up and Loading Configuration File' on page 558).</li> <li>▪ <b>Reset:</b> Opens the Maintenance Actions page for performing various maintenance procedures such as resetting the device (see 'Resetting the Device' on page 529).</li> <li>▪ <b>Software Upgrade Wizard:</b> starts the Software Upgrade wizard for upgrading the device's software (see 'Software Upgrade Wizard' on page 555).</li> </ul>
	<b>Home</b>	Opens the Home page (see 'Viewing the Home Page' on page 54).
	<b>Help</b>	Opens the Online Help topic of the currently opened configuration page (see 'Getting Help' on page 53).
	<b>Log off</b>	Logs off a session with the Web interface (see 'Logging Off the Web Interface' on page 54).



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

**Figure 7-3: "Reset" Displayed on Toolbar**



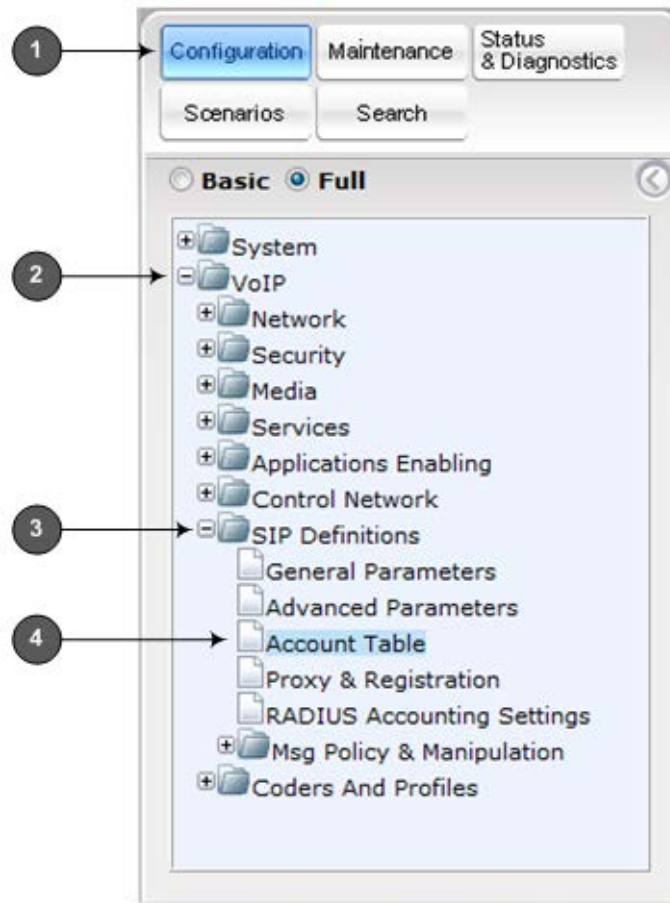
## 7.1.5 Navigation Tree

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

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

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

Figure 7-4: Navigating in Hierarchical Menu Tree (Example)



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

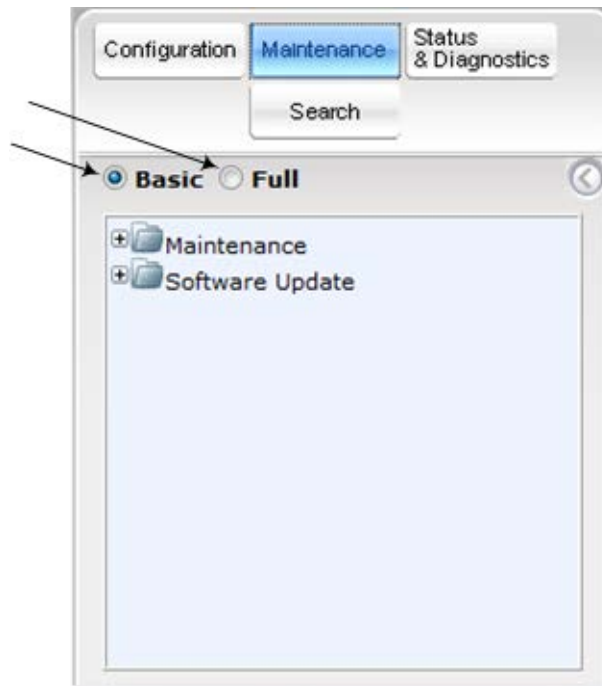
#### 7.1.5.1 Displaying Navigation Tree in Basic and Full View

You can view an expanded or reduced display of the Navigation tree. This affects the number of displayed menus and submenus in the tree. The expanded (*Full*) view displays all the menus pertaining to the selected configuration tab; the reduced (*Basic*) view displays only commonly used menus. This is relevant when using the configuration tabs (i.e., **Configuration**, **Maintenance**, and **Status & Diagnostics**) on the Navigation bar. The advantage of the Basic view is that it prevents "cluttering" of the Navigation tree with menus that may not be required.

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

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

Figure 7-5: Basic and Full View Options



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

### 7.1.5.2 Showing / Hiding the Navigation Pane

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

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



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

Figure 7-6: Show and Hide Button (Navigation Pane in Hide View)







## 7.1.6 Working with Configuration Pages

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

### 7.1.6.1 Accessing Pages

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

➤ **To open a configuration page:**

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

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



**Notes:**

- You can also access certain pages from the **Device Actions** button located on the toolbar (see 'Toolbar Description' on page 41).
- To view all the menus in the Navigation tree, ensure that the Navigation tree is in Full view (see 'Displaying Navigation Tree in Basic and Full View' on page 43).
- To get Online Help for the currently displayed page, see 'Getting Help' on page 53.
- Certain pages may not be accessible or may be read-only, depending on the access level of your Web user account (see 'Configuring Web User Accounts' on page 58). If a page is read-only, "Read-Only Mode" is displayed at the bottom of the page.

### 7.1.6.2 Viewing Parameters

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

- Displaying "basic" and "advanced" parameters - see 'Displaying Basic and Advanced Parameters' on page 45
- Displaying parameter groups - see 'Showing / Hiding Parameter Groups' on page 46

#### 7.1.6.2.1 Displaying Basic and Advanced Parameters

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

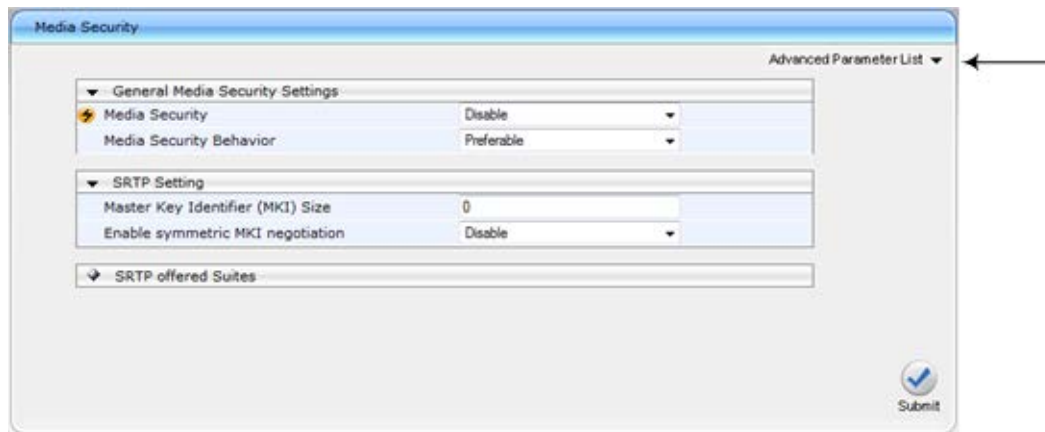
- **Advanced Parameter List** button with down-pointing arrow: click this button to

display all parameters.

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

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

**Figure 7-7: Toggling between Basic and Advanced View**



**Notes:**

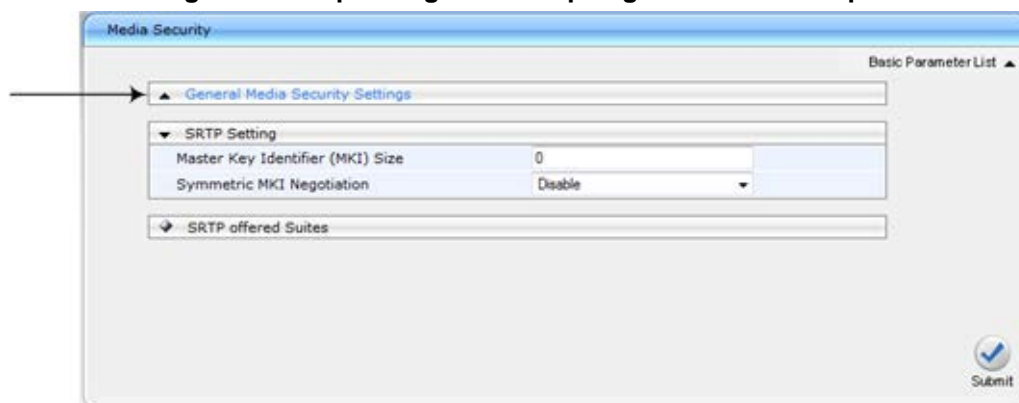
- When the Navigation tree is in Full mode (see 'Navigation Tree' on page 42), configuration pages display all their parameters.
- If a page contains only basic parameters, the **Basic Parameter List** button is not displayed.
- If you reset the device, the Web pages display only the basic parameters.
- The basic parameters are displayed in a dark blue background.





### 7.1.6.2.2 Showing / Hiding Parameter Groups

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

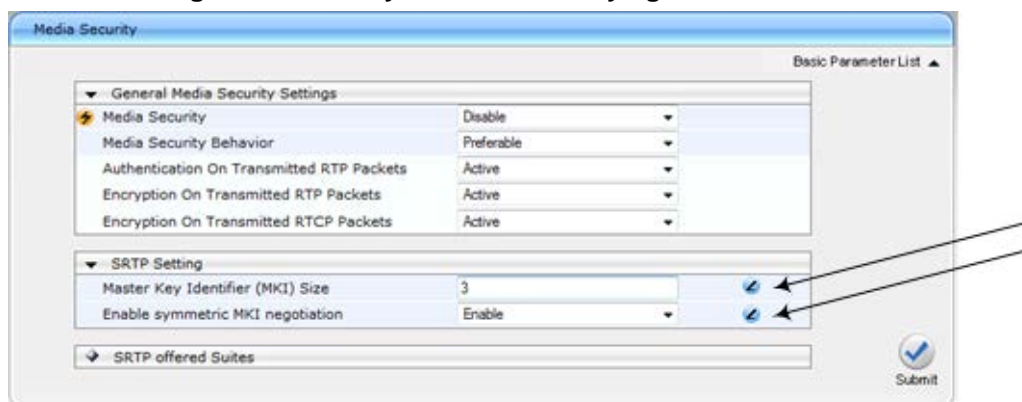
**Figure 7-8: Expanding and Collapsing Parameter Groups**





### 7.1.6.3 Modifying and Saving Parameters


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

**Figure 7-9: Edit Symbol after Modifying Parameter Value**



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

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

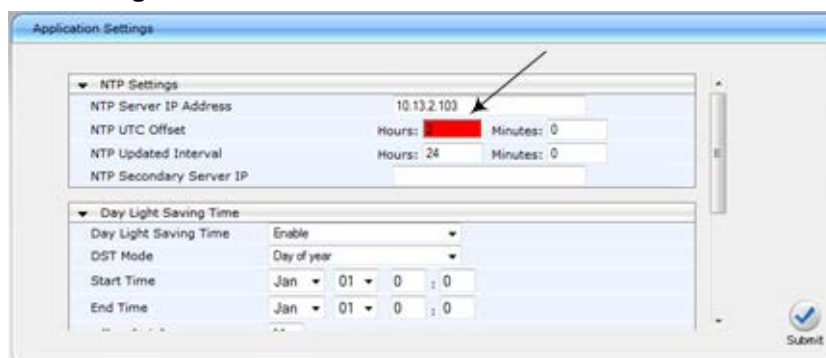
When you click **Submit**, modifications to parameters with on-the-fly capabilities are immediately applied to the device and take effect. Parameters displayed on the page with the lightning  symbol take effect only after a device reset. For resetting the device, see 'Resetting the Device' on page 529.



**Note:** Parameters saved to the volatile memory (by clicking **Submit**), revert to their previous settings after a hardware or software reset, or if the device is powered down. Therefore, to ensure parameter changes (whether on-the-fly or not) are retained, save ('burn') them to the device's non-volatile memory, i.e., flash (see 'Saving Configuration' on page 532).

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

Figure 7-10: Value Reverts to Previous Valid Value



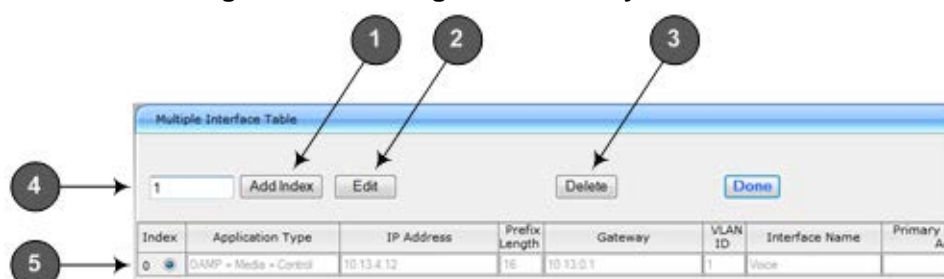
## 7.1.6.4 Working with Tables

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

### 7.1.6.4.1 Basic Design Tables

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

Figure 7-11: Adding an Index Entry to a Table



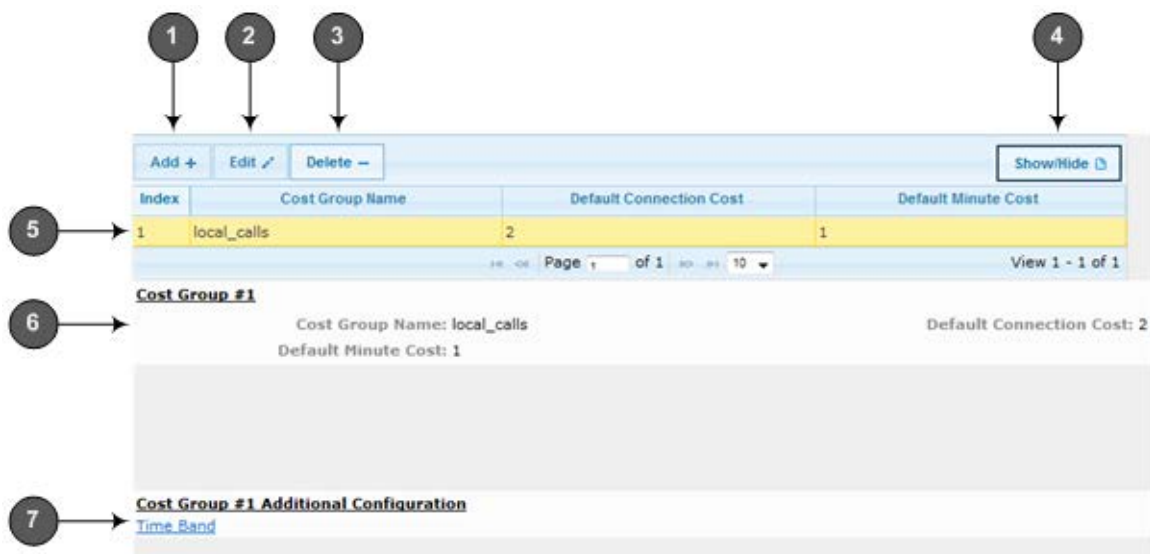
Basic Table Design Description

Item #	Button / Field	
1	<b>Add Index</b> (or <b>Add</b> ) button	Adds an index entry row to the table.
2	<b>Edit</b>	Edits the selected row.
3	<b>Delete</b>	Removes the selected row from the table.
4	'Add Index' field	Defines the index number. When adding a new row, enter the required index number in this field, and then click <b>Add Index</b> .
5	<b>Index</b> radio button	Selects the row for editing and deleting.
-	<b>Compact</b> button	Organizes the index entries in ascending, consecutive order, starting from index 0. For example, assume you have three index entries, 0, 4 and 6. After you click <b>Compact</b> , index entry 4 is re-assigned to index 1 and index entry 6 is re-assigned to index 2.
-	<b>Apply</b> button	Saves the row configuration. Click this button after you add or edit each index entry.

#### 7.1.6.4.2 Enhanced Design Tables

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

Figure 7-12: Displayed Details Pane



Enhanced Table Design Description

Item #	Button	
1	<b>Add</b>	Adds a new index entry row to the table. When you click this button, a dialog box appears with parameters for configuring the new entry. When you have completed configuration, click the <b>Submit</b> button in the dialog box to add it to the table.
2	<b>Edit</b>	Edits the selected row.
3	<b>Delete</b>	Removes the selected row from the table. When you click this button, a confirmation box appears requesting you to confirm deletion. Click <b>Delete</b> to accept deletion. <div data-bbox="746 1447 1232 1666"> </div>
4	<b>Show/Hide</b>	Toggles between displaying and hiding the full configuration of a selected row. This configuration is displayed below the table (see Item #6) and is useful for large tables that cannot display all its columns in the work pane.
5	-	Selected index row entry for editing, deleting and showing configuration.
6	-	Displays the full configuration of the selected row when you click the <b>Show/Hide</b> button.

Item #	Button	
7	-	Links to access additional configuration tables related to the current configuration.

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

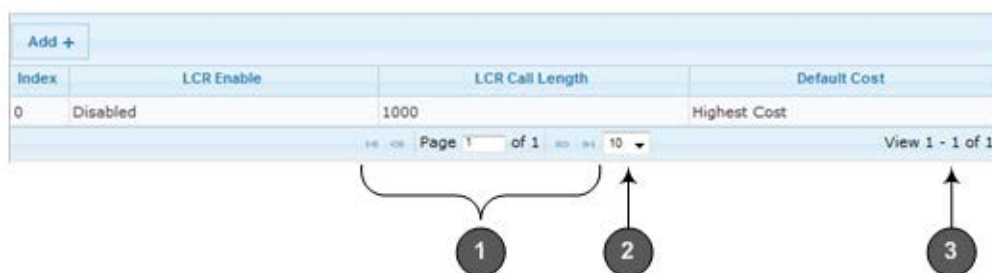
**Figure 7-13: Invalid Configuration with Index Highlighted in Red**



Add +			
Index	Cost Group Name	Default Connection Cost	Default Minute Cost
7	local_calls	2	1
Page 1 of 1			

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

**Figure 7-14: Viewing Table Rows per Page**



Add +			
Index	LCR Enable	LCR Call Length	Default Cost
0	Disabled	1000	Highest Cost
Page 1 of 1			

**Row Display and Page Navigation**

Item #	Description
1	Defines the page that you want to view. Enter the required page number or use the following page navigation buttons: <ul style="list-style-type: none"> <li>Next - Displays the next page</li> <li>Previous - Displays the last page</li> <li>First - Displays the previous page</li> <li>Last - Displays the first page</li> </ul>
2	Defines the number of rows to display per page. You can select 5 or 10, where the default is 10.
3	Displays the currently displayed page number.

## 7.1.7 Searching for Configuration Parameters

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

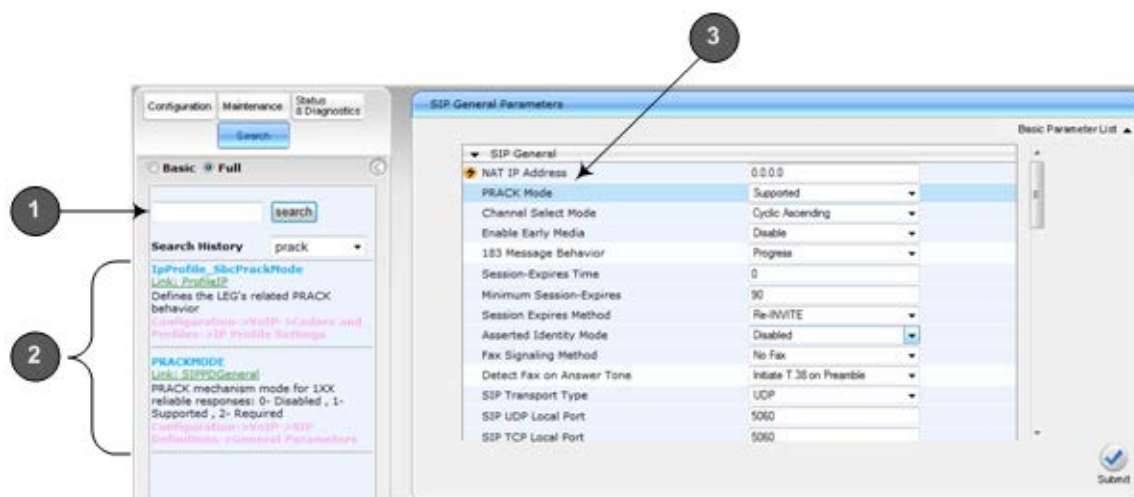


**Note:** If an *ini* file parameter is not configurable in the Web interface, the search fails.

➤ **To search for a parameter:**

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

**Figure 7-15: Searched Result Screen**



**Search Description**

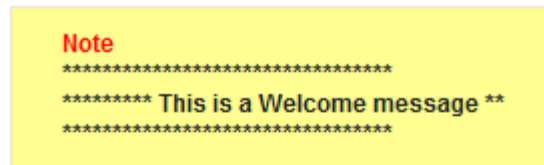
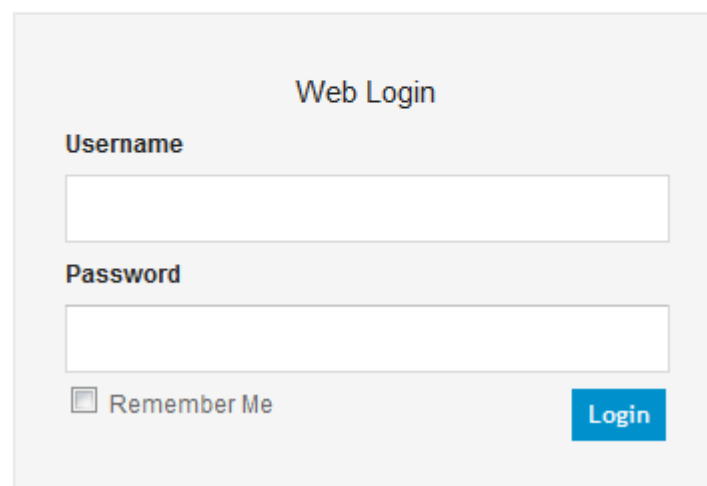
Item #	Description
1	Search field for entering search key and <b>Search</b> button for activating the search process.
2	Search results listed in Navigation pane.
3	Found parameter, highlighted on relevant Web page



## 7.1.8 Creating a Login Welcome Message

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

**Figure 7-16: User-Defined Web Welcome Message after Login**

Web Login

**Username**

**Password**

☐ Remember Me **Login**

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

### **ini File Parameter for Welcome Login Message**

Parameter	Description
<b>[WelcomeMessage]</b>	<p>Enables and defines a Welcome message that appears on the Web Login page for logging in to the Web interface.</p> <p>The format of this parameter is as follows:</p> <pre>[WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; [WelcomeMessage]</pre> <p>For Example:</p> <pre>[WelcomeMessage ] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; WelcomeMessage 1 = "*****", WelcomeMessage 2 = "***** This is a Welcome message ****", WelcomeMessage 3 = "*****", [WelcomeMessage]</pre> <p>Each index row represents a line of text in the Welcome message box. Up to 20 lines (or rows) of text can be defined.</p>



## 7.1.9 Getting Help

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

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


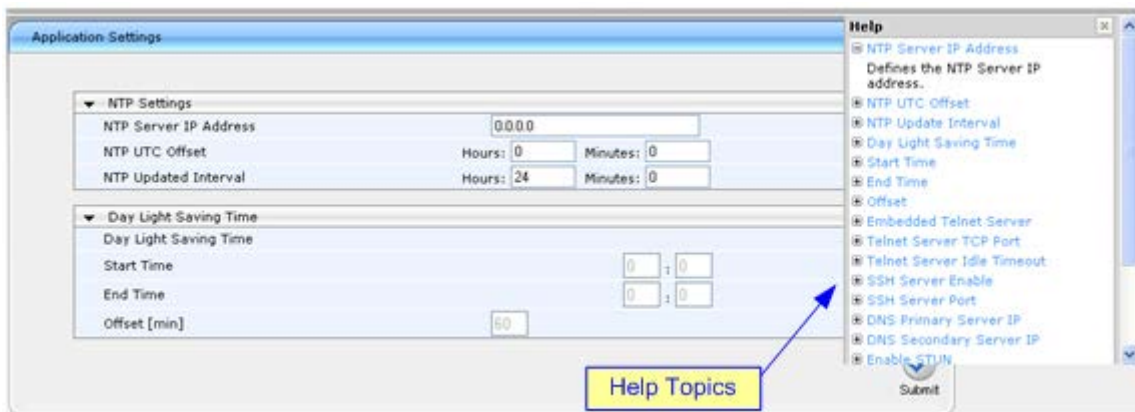




1. On the toolbar, click the **Help**  button; the Help topic pertaining to the opened page appears, as shown below:

Figure 7-17: Help Topic for Current Page



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



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

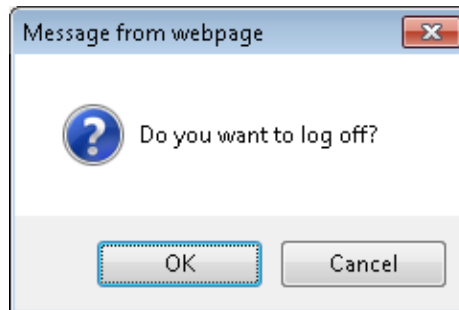
## 7.1.10 Logging Off the Web Interface

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

### ➤ To log off the Web interface:

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

**Figure 7-18: Log Off Confirmation Box**



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

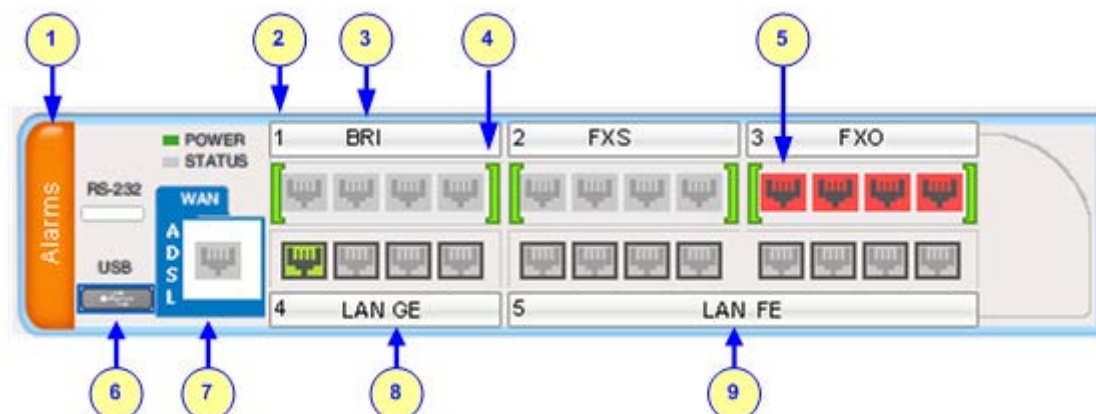
## 7.2 Viewing the Home Page

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

### ➤ To access the Home page:

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

**Figure 7-19: Home Page**



**Note:** The displayed number and type of telephony interfaces, LAN interfaces and WAN interfaces depends on the ordered hardware configuration.






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












- **IP Address:** IP address of the device
- **Subnet Mask:** Subnet mask address of the device
- **Default Gateway Address:** Default gateway used by the device
- **Digital Port Number:** Number of digital PRI ports (depending on ordered hardware configuration)
- **BRI Port Number:** Number of BRI ports (depending on ordered hardware configuration))
- **Analog Port Number:** Number of analog (FXS, FXO) ports (depending on ordered hardware configuration)
- **Firmware Version:** Software version running on the device
- **Protocol Type:** Signaling protocol currently used by the device (i.e. SIP)
- **Gateway Operational State:**
  - "LOCKED": device is locked (i.e. no new calls are accepted)
  - "UNLOCKED": device is not locked
  - "SHUTTING DOWN": device is currently shutting down








To perform these operations, see 'Basic Maintenance' on page [529](#).

The table below describes the areas of the Home page.

**Home Page Description**

Item #	Description		
1	Displays the highest severity of an active alarm raised (if any) by the device: <ul style="list-style-type: none"> <li>■ Green = No alarms</li> <li>■ Red = Critical alarm</li> <li>■ Orange = Major alarm</li> <li>■ Yellow = Minor alarm</li> </ul> To view active alarms, click the Alarms area to open the Active Alarms page (see Viewing Active Alarms on page <a href="#">579</a> ).		
2	Module slot number.		
3	Module interface type (e.g., FXS, FXO, and DIGITAL).		
4	Module status icon: <ul style="list-style-type: none"> <li>■  (green): Module has been inserted or is correctly configured</li> <li>■  (gray): Module was removed and "Reserved" is displayed</li> <li>■  (red): Module failure and "Failure" is displayed</li> </ul>		
5	Port (trunk or channel) status icon.		
	<b>Icon</b>	<b>Trunk Description (Digital Module)</b>	<b>Channel Description (Analog Modules)</b>
	 (gray)	Disable: Trunk not configured (not in use)	Idle: Channel is currently on-hook
		Active - OK: Trunk	Call Connected: Active RTP stream

Item #	Description		
	(green)	synchronized	
	 (yellow)	RAI Alarm: Remote Alarm Indication (RAI), also known as the Yellow Alarm	-
	 (red)	LOS/LOF Alarm: Loss due to LOS (Loss of Signal) or LOF (Loss of Frame)	Not Connected: No FXO line is connected to this port or port out of service due to Serial Peripheral Interface (SPI) failure (applicable only to FXO interfaces)
	 (blue)	AIS Alarm: Alarm Indication Signal (AIS), also known as the Blue Alarm	Handset Offhook: Channel is off-hook, but there is no active RTP session
	 (orange)	D-Channel Alarm: D-channel alarm	-
	 (dark orange)	NFAS Alarm	-
	<p>If you click a port, a shortcut menu appears with commands allowing you to do the following:</p> <ul style="list-style-type: none"> <li>Reset channel (Analog ports only): Resets the analog port (see Resetting an Analog Channel on page 533)</li> <li>Port Settings: Displays trunk status (see 'Viewing Trunk and Channel Status' on page 589) and analog port status (see 'Viewing Analog Port Information' on page 590)</li> <li>Update Port Info: Assigns a name to the port (see 'Assigning a Port Name' on page 57)</li> </ul>		
6	<p>USB port for 3G cellular WAN modem for primary or backup WAN:</p> <ul style="list-style-type: none"> <li>Gray - USB 3G cellular modem is not configured.</li> <li>Blue - USB 3G cellular modem is in standby mode (backup mode).</li> <li>Green - USB 3G cellular modem is active.</li> <li>Red - USB 3G cellular modem is not active</li> </ul>		
7	<p>WAN port status icons:</p> <ul style="list-style-type: none"> <li> (green): Link is working</li> <li> (gray): Link is not configured</li> <li> (red): Link error</li> </ul> <p>Depending on ordered hardware configuration, the WAN port can be Gigabit Ethernet copper, SHDSL, or ADSL2+ / VDSL2:</p> <div style="display: flex; justify-content: space-around; align-items: flex-end;"> <div style="text-align: center;"> <p>Gigabit Ethernet</p>  <p>One Port</p> </div> <div style="text-align: center;"> <p>SHDSL</p>  <p>Four Ports</p> </div> <div style="text-align: center;"> <p>ADSL2+ / VDSL2</p>  <p>One Port</p> </div> </div>		

Item #	Description
8	<p>Gigabit Ethernet LAN port status icons:</p> <ul style="list-style-type: none"> <li> (green): Link is working</li> <li> (gray): Link is not configured</li> <li> (red): Link error</li> </ul> <p>To view detailed port information, click the port icon (see Viewing Ethernet Port Information on page 577).</p>
9	Fast Ethernet LAN port status icons. See Item 8 for a description.
8 & 9	<p>Power-over-Ethernet status for LAN ports:</p> <ul style="list-style-type: none"> <li> (gray with dark gray frame): Link is not connected</li> <li> (green with dark gray frame): Ethernet delivered</li> <li> (gray with orange frame): Power delivered</li> <li> (green with orange frame): Ethernet and power delivered</li> </ul>

## 7.2.1 Assigning a Port Name

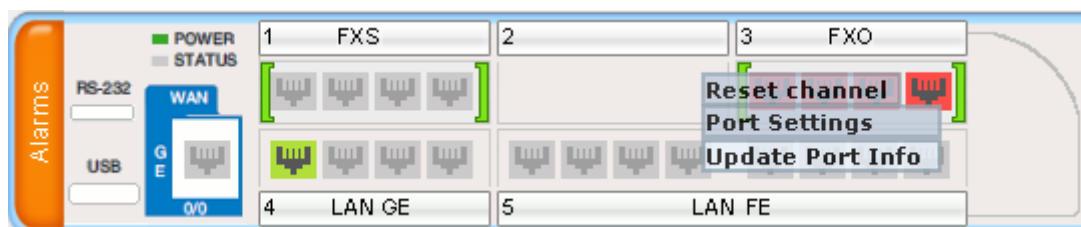
The Home page allows you to assign an arbitrary name or a brief description to each port. This description appears as a tooltip when you move your mouse over the port.



**Note:** Only alphanumeric characters can be used in the port description.

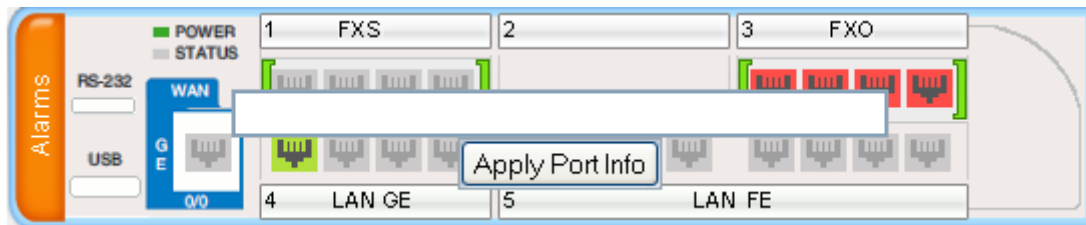
### ➤ To add a port description:

1. Click the required port icon; a shortcut menu appears, as shown below:



2. From the shortcut menu, choose **Update Port Info**; a text box appears.

Figure 7-20: Text Box for Entering Port Name



3. Type a brief description for the port, and then click **Apply Port Info**.

## 7.3 Configuring Web User Accounts

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

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

Access Levels of Web User Accounts

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

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

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

**Pre-configured Web User Accounts**

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

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

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

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

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

**Notes:**

- For security, it's recommended that you change the default username and password.
- The Security Administrator user can change all attributes of all Web user accounts. Web users with access levels other than Security Administrator can change only their password and username.
- To restore the two Web user accounts to default settings (usernames and passwords), set the *ini* file parameter ResetWebPassword to 1.
- To log in to the Web interface with a different Web user, click the **Log off** button and then login with with a different username and password.
- You can set the entire Web interface to read-only (regardless of Web user access levels), by using the *ini* file parameter DisableWebConfig (see 'Web and Telnet Parameters' on page 668).
- You can define additional Web user accounts using a RADIUS server.



### 7.3.1 Basic User Accounts Configuration

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

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


**Notes:**

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

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

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

**Figure 7-21: WEB User Accounts Page (for Users with 'Security Administrator' Privileges)**

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

2. To change the username of an account:
  - a. In the 'User Name' field, enter the new user name.
  - b. Click **Change User Name**; if you are currently logged in to the Web interface with this account, the 'Web Login' dialog box appears.
  - c. Log in with your new user name.
3. To change the password of an account:
  - a. In the 'Current Password' field, enter the current password.
  - b. In the 'New Password' and 'Confirm New Password' fields, enter the new password.
  - c. Click **Change Password**; if you are currently logged in to the Web interface with this account, the 'Web Login' dialog box appears.
  - d. Log in with your new password.



4. To change the access level of the optional, second account:
  - a. Under the **Account Data for User: User** group, from the 'Access Level' drop-down list, select a new access level user.
  - b. Click **Change Access Level**; the new access level is applied immediately.

### 7.3.2 Advanced User Accounts Configuration

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

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

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



#### Notes:

- Only the Security Administrator user can **initially** access the Web Users table.
- Only Security Administrator and Master users can add, edit, or delete users.
- Admin users have read-only privileges in the Web Users table. Monitor users have no access to this page.
- If you delete a user who is currently in an active Web session, the user is immediately logged off by the device.
- All users can change their own passwords. This is done in the WEB Security Settings page (see 'Configuring Web Security Settings' on page 65).
- To remove the Web Users table and revert to the Web User Accounts page with the pre-configured, default Web user accounts, set the ResetWebPassword *ini* file parameter to 1. This also deletes all other Web users.
- Once the Web Users table is accessed, Monitor users and Admin users can only change their passwords in the Web Security Settings page (see 'Configuring Web Security Settings' on page 65). The new password must have at least four different characters than the previous password. (The Security Administrator users and Master users can change their passwords in the Web Users table and in the Web Security Settings page.)
- This table can only be configured using the Web interface or CLI command web-users.

➤ **To add Web user accounts with advanced settings:**

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

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

**Figure 7-22: Web Users Table Page**

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

Page 1 of 1    View 1 - 2 of 2

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

**Figure 7-23: Web Users Table - Add Record Dialog Box**

**Add Record**
✕

Index

Username

Password

Status

New ▼

Password Age

Session Limit

Session Timeout

Block Duration

User Level

Monitor ▼

Submit

✕ Cancel

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

**Web User Parameters Description**

Parameter	Description
Web: Username CLI: user-name	Defines the Web user's username. The valid value is a string of up to 40 alphanumeric characters, including the period ".", underscore "_", and hyphen "-" signs.
Web: Password CLI: password	Defines the Web user's password. The valid value is a string of 8 to 40 ASCII characters, which must include the following: <ul style="list-style-type: none"> <li>▪ At least eight characters</li> <li>▪ At least two letters that are upper case (e.g., "AA")</li> <li>▪ At least two letters that are lower case (e.g., "aa")</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>At least two numbers</li> <li>At least two signs (e.g., the dollar "\$" sign)</li> <li>No spaces in the string</li> <li>At least four characters different to the previous password</li> </ul>
Web: Status CLI: status	<p>Defines the status of the Web user.</p> <ul style="list-style-type: none"> <li>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.</li> <li>Valid = User can log in to the Web interface as normal.</li> <li>Failed Access = This state is automatically set for users that exceed a user-defined number of failed login attempts, set by the 'Deny Access on Fail Count' parameter (see 'Configuring Web Security Settings' on page 65). These users can log in only after a user-defined timeout configured by the 'Block Duration' parameter (see below) or if their status is changed (to New or Valid) by a System Administrator or Master.</li> <li>Old Account = This state is automatically set for users that have not accessed the Web interface for a user-defined number of days, set by the 'User Inactivity Timer' (see 'Configuring Web Security Settings' on page 65). 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.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The Old Account status is applicable only to Admin and Monitor users; System Administrator and Master users can be inactive indefinitely.</li> <li>For security, it is recommended to set the status of a newly added user to New in order to enforce password change.</li> </ul>
Web: Password Age CLI: pw-age-interval	<p>Defines the duration (in days) of the validity of the password. When this duration elapses, the user is prompted to change the password; otherwise, access to the Web interface is blocked.</p> <p>The valid value is 0 to 10000, where 0 means that the password is always valid. The default is 90.</p>
Web: Session Limit CLI: session-limit	<p>Defines the maximum number of Web interface sessions allowed for the user. In other words, this allows the same user account to log in to the device from different sources (i.e., IP addresses).</p> <p>The valid value is 0 to 5. The default is 2.</p> <p><b>Note:</b> Up to 5 users can be logged in to the Web interface at any given.</p>
Web: Session Timeout CLI: session-timeout	<p>Defines the duration (in minutes) of Web inactivity of a logged-in user, after which the user is automatically logged off the Web interface.</p> <p>The valid value is 0 to 100000. The default value is according to the settings of the 'Session Timeout' global parameter (see 'Configuring Web Security Settings' on page 65).</p>

Parameter	Description
Web: Block Duration CLI: block-time	<p>Defines the duration (in seconds) for which the user is blocked when the user exceeds a user-defined number of failed login attempts. This is configured by the 'Deny Access On Fail Count' parameter (see 'Configuring Web Security Settings' on page 65).</p> <p>The valid value is 0 to 100000, where 0 means that the user can do as many login failures without getting blocked. The default is according to the settings of the 'Deny Authentication Timer' parameter (see 'Configuring Web Security Settings' on page 65).</p> <p><b>Note:</b> The 'Deny Authentication Timer' parameter relates to failed Web logins from specific IP addresses.</p>
Web: User Level CLI: user-level	<p>Defines the user's access level.</p> <ul style="list-style-type: none"> <li>Monitor = (Default) Read-only user. This user can only view Web pages and access to security-related pages is denied.</li> <li>Admin = Read/write privileges for all pages, except security-related pages including the Web Users table where this user has only read-only privileges.</li> <li>SecAdmin = Read/write privileges for all pages. This user is the Security Administrator.</li> <li>Master-User = Read/write privileges for all pages. This user also functions as a security administrator.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>At least one Security Administrator must exist. The last remaining Security Administrator cannot be deleted.</li> <li>The first Master user can be added only by a Security Administrator user.</li> <li>Additional Master users can be added, edited and deleted only by Master users.</li> <li>If only one Master user exists, it can be deleted only by itself.</li> <li>Master users can add, edit, and delete Security Administrators (but cannot delete the last Security Administrator).</li> <li>Only Security Administrator and Master users can add, edit, and delete Admin and Monitor users.</li> </ul>

## 7.4 Displaying Login Information upon Login

The device can display login information immediately upon Web login.

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

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

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

Figure 7-24: Login Information Window

Login Information	
Last Login Privilege	Security Administrator
Last Failed Login Time	15: 04: 19
Last Failed Login Date	10/06/2012
Last Failed Login IP	10.13.2.11
Login Attempts Since Last Success	2
Last Success Login Time	15: 03: 32
Last Success Login Date	10/06/2012
Last Success Login IP	10.13.2.11

Close

## 7.5 Configuring Web Security Settings

The WEB Security Settings page is used to define a secure Web access communication method. For a description of these parameters, see 'Web and Telnet Parameters' on page 668.

➤ **To define Web access security:**

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

Figure 7-25: Web Security Settings Page

<b>General</b>	
HTTP Authentication Mode	Web Based Authentication ▼
Secured Web Connection (HTTPS)	HTTP and HTTPS ▼
Requires Client Certificates for HTTPS connection	Disable ▼
HTTPS Cipher String	RC4:EXP
WAN OAMP Interface	Not Configured ▼
Allow WAN access to HTTP	Disable ▼
Allow WAN access to HTTPS	Disable ▼
<b>Session</b>	
Session Timeout (minutes)	15
<b>Access Block Parameters</b>	
Deny Authentication Timer	60
Deny Access On Fail Count	3 ▼
Display Login Information	No ▼

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 7.6 Limiting OAMP Access to a Specific WAN Interface

You can limit the access of OAMP applications (such as HTTP, HTTPS, Telnet, and SSH) to a specific WAN interface. This OAMP-interface binding can then be associated with a Virtual Routing and Forwarding (VRF).

➤ **To limit OAMP access on a specific WAN interface, using CLI.**

1. Enable WAN management access for specific OAMP applications, using any of the following commands:

```
set wan-ssh-allow
set wan-telnet-allow
set wan-snmp-allow
set wan-http-allow
set wan-https-allow
```

2. Define the WAN interface for the OAMP applications, using the OAMPWanInterfaceName ini file parameter or the following CLI command:

```
bind GigabitEthernet <slot/port.vlanId> oamp
bind vlan <vlanId> oamp
```

The following example enables WAN access for Telnet on interface GigabitEthernet 0/0.4 (GigabitEthernet 0/0.4 may be associated with a VRF):

```
(config-system)# cli-terminal
(cli-terminal)# set wan-telnet-allow on
(cli-terminal)# exit
(config-system)# bind GigabitEthernet 0/0.5 oamp
```

➤ **To define the WAN OAMP interface using the Web interface:**

1. Open the WEB Security Settings page (see 'Configuring Web Security Settings' on page 65).
2. From the 'WAN OAMP Interface' drop-down list, select the required WAN interface.
3. Click **Submit** to apply your changes.

## 7.7 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.

## 7.8 Configuring Web and Telnet Access List

The Web & Telnet Access List page is used to define IP addresses (up to ten) that are permitted to access the device's Web, Telnet, and SSH interfaces. Access from an undefined IP address is denied. If no IP addresses are defined, this security feature is inactive and the device can be accessed from any IP address. The Web and Telnet Access List can also be defined using the *ini* file parameter `WebAccessList_x` (see 'Web and Telnet Parameters' on page 668).

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

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

**Figure 7-26: Web & Telnet Access List Page - Add New Entry**

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

**Figure 7-27: Web & Telnet Access List Table**

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

3. To delete authorized IP addresses, select the Delete Row check boxes corresponding to the IP addresses that you want to delete, and then click **Delete Selected Addresses**; the IP addresses are removed from the table and these IP addresses can no longer access the Web and Telnet interfaces.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.


**Notes:**

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

## 7.9 Configuring RADIUS Settings

The RADIUS Settings page is used for configuring the Remote Authentication Dial In User Service (RADIUS) accounting parameters. For a description of these parameters, see 'Configuration Parameters Reference' on page 661.

➤ **To configure RADIUS:**

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

**Figure 7-28: RADIUS Parameters Page**

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

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.



## 8 CLI-Based Management

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



### Notes:

- For security, CLI is disabled by default.
- For information on accessing the CLI interface through the RS-232 port interface, see 'CLI' on page 27.
- For more information on the CLI commands, refer to the following documents:
  - MSBR Series CLI Reference Guide for Data Functionality
  - MSBR Series CLI Reference Guide for System and VoIP Functionality

### 8.1 Enabling CLI using Telnet

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

For security, some organizations require the display of a proprietary notice upon starting a Telnet session. You can use the configuration ini file parameter, WelcomeMessage to configure such a message (see Creating a Login Welcome Message on page 52).

#### ➤ To enable Telnet:

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

Figure 8-1: Telnet Settings on Telnet/SSH Settings Page

▼ Telnet Settings	
Embedded Telnet Server	Enable Unsecured ▼
Telnet Server TCP Port	23
⚡ Telnet Server Idle Timeout	60
⚡ Allow WAN access to Telnet	Enable ▼

2. Set the 'Embedded Telnet Server' parameter to **Enable Unsecured** or **Enable Secured** (i.e, SSL).
3. To enable Telnet from the WAN, set the 'Allow WAN access to Telnet' parameter to **Enable**.
4. Configure the other Tenet parameters as required. For a description of these parameters, see Telnet Parameters on page 671.
5. Click **Submit**.
6. Save the changes to flash memory with a device reset.

## 8.2 Enabling CLI using SSH and RSA Public Key

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

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

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

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

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

**Figure 8-2: Selecting Public RSA Key in PuTTY**



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

**Figure 8-3: SSH Settings - Pasting Public RSA Key in 'Admin Key' Field**

SSH Settings	
Enable SSH Server	Enable
Server Port	22
Admin Key	AAAAB3NzaC1yc2EAAAABJQAAAIB
Require Public Key	Enable
Max Payload Size	32768
Max Binary Packet Size	35000
Enable Last Login Message	Enable
Max Login Attempts	3
Allow WAN access to SSH	Disable

- c. For additional security, you can set the 'Require Public Key' to **Enable**. This ensures that SSH access is only possible by using the RSA key and not by using user name and password.
    - d. To enable SSH from the WAN, set 'Allow WAN access to SSH' to **Enable**.
    - e. Configure the other SSH parameters as required. For a description of these parameters, see SSH Parameters on page 692.
    - f. Click **Submit**.
  3. Start the PuTTY Configuration program, and then do the following:
    - a. In the 'Category' tree, drill down to **Connection**, then **SSH**, and then **Auth**; the 'Options controlling SSH authentication' pane appears.
    - b. Under the 'Authentication parameters' group, click **Browse** and then locate the private key file that you created and saved in Step 4.
  4. Connect to the device with SSH using the username "Admin"; RSA key negotiation occurs automatically and no password is required.
- **To configure RSA public keys for Linux (using OpenSSH 4.3):**
1. Run the following command to create a new key in the admin.key file and to save the public portion to the admin.key.pub file:
 

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

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

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

## 8.3 Establishing a CLI Session

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



### Notes:

- The default login username and password are both "Admin" (case-sensitive).
- Only the primary User Account, which has Security Administration access level (200) can access the device using Telnet. For configuring the username and password, see [Configuring Web User Accounts](#) on page 58.

### ➤ To establish a CLI session with the device:

1. Establish a Telnet or SSH session with the device using its OAMP IP address.
2. Log in to the session using the username and password assigned to the Admin user of the Web interface:

3. At the Username prompt, type the username, and then press Enter:

```
Username: Admin
```

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

```
Password: Admin
```

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

```
enable
```

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

```
Password: Admin
```

Once logged in, you can configure the device by accessing one of the following modes:

- **Basic:** Provides general CLI commands, for example, to display system information and activate debugging. This mode is accessed immediately after you login to the CLI. For example, to access the command shell, type the following command, and then press Enter:

```
cmdshell
```

- **Enable:** Provides the configuration commands and is accessed by typing the following command:

```
# enable
```

```
# Password: <password>
```

This mode groups the commands under the following command sets:

- **configure-system:** This contains the general and system related configuration commands, for example, Syslog configuration. This set is accessed by typing the following:

```
# configure system
```

- **configure-data:** This contains the data-router configuration commands. This set is accessed by typing the following:

```
# configure data
```

- **configure-voip:** This contains VoIP-related configuration commands, for example, SIP, VoIP network interfaces, and VoIP media configurations. This set is accessed by typing the following:

```
# configure voip
```

## 8.4 Configuring TACACS+ for CLI Login

This section describes how to enable and configure Terminal Access Controller Access-Control System (TACACS+). TACACS+ is a security protocol for centralized username and password verification. TACACS+ can be used for validating users attempting to gain access to the device through CLI. TACACS+ services are maintained on a database on a TACACS+ daemon. You must have access to and must configure a TACACS+ server before configuring TACACS+ on your device.

TACACS+ can provide the following services:

- Authentication: provides authentication through login and password dialog
- Authorization: manages user capabilities for the duration of the user's session by placing restrictions on what commands a user may execute
- Accounting: collects and sends information for auditing and reporting to the TACACS+ daemon

The TACACS+ protocol provides authentication between the device and the TACACS+ daemon, and it ensures confidentiality as all protocol exchanges between a network access server and a TACACS+ daemon are encrypted. You need a system running TACACS+ daemon software to use the TACACS+ functionality on your network access server.

When a user attempts a simple ASCII login by authenticating to a network access server using TACACS+, the following typically occurs:

1. When the connection is established, the network access server contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the user. The user enters a username and the network access server then contacts the TACACS+ daemon to obtain a password prompt. The network access server displays the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ daemon.
2. The network access server eventually receives one of the following responses from the TACACS+ daemon:
  - ACCEPT: The user is authenticated and service may begin. If the network access server is configured to require authorization, authorization will begin at this time.
  - REJECT: The user has failed to authenticate. The user may be denied further access.
  - ERROR: An error occurred at some time during authentication. This can be at the daemon or in the network connection between the daemon and the network access server. If an ERROR response is received, the device typically attempts to use an alternative method for authenticating the user.
3. If TACACS+ authorization is needed, the TACACS+ daemon is again contacted for each CLI command entered by the user, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the CLI command is allowed; otherwise, it is rejected.

The following CLI commands are used for enabling and configuring TACACS+:

- **aaa authentication login tacacs+**: enables TACACS+
- **tacacs-server host <host-ip>**: defines the IP address of the TACACS+ server (up to two servers can be configured)
- **tacacs-server port <port-num>**: defines the TCP port number for the TACACS+ service
- **tacacs-server key <password>**: defines the shared secret between the TACACS+ server and the device
- **tacacs-server timeout <seconds>**: defines how much time to wait for a TACACS+ response before failing the authentication

The procedure below describes how to configure TACACS+ through CLI.

➤ **To configure TACACS+ through the CLI:**

1. Establish serial communication with the device.
2. At the prompt, type the following command to access the data interface and then press Enter:

```
# configure data
```

3. At the prompt, type the TACACS+ commands, as required, to enable and configure TACACS+. Below shows an example configuration:

```
(config-data)# aaa authentication login tacacs+
(config-data)# tacacs-server host 192.168.1.55
(config-data)# tacacs-server key Tumble
```

## 9 SNMP-Based Management

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

This section provides configuration relating to SNMP management.



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

### 9.1 Configuring SNMP Community Strings

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

For detailed descriptions of the SNMP parameters, see 'SNMP Parameters' on page 672.

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

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

**Figure 9-1: SNMP Community String Page**

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

▼	
⚡ Disable SNMP	No ▼
Trap Community String	trapuser
Trap Manager Host Name	
⚡ Allow WAN access to SNMP	Disable ▼

2. Configure the SNMP community strings parameters according to the table below.
  3. Click **Submit** to apply your changes.
  4. To save the changes to flash memory, see 'Saving Configuration' on page 532.
- To delete a community string, select the **Delete** check box corresponding to the community string that you want to delete, and then click **Submit**.

**SNMP Community String Parameters Description**

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

## 9.2 Configuring SNMP Trap Destinations

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

➤ **To configure SNMP trap destinations:**

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

**Figure 9-2: SNMP Trap Destinations Page**

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

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



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



## SNMP Trap Destinations Parameters Description

Parameter	Description
Web: SNMP Manager [SNMPManagerIsUsed_x]	Enables the SNMP Manager to receive traps and checks the validity of the configured destination (IP address and port number). <ul style="list-style-type: none"> <li>[0] (check box cleared) = (Default) Disables SNMP Manager</li> <li>[1] (check box selected) = Enables SNMP Manager</li> </ul>
Web: IP Address [SNMPManagerTableIP_x]	Defines the IP address (in dotted-decimal notation, e.g., 108.10.1.255) of the remote host used as the SNMP Manager. The device sends SNMP traps to this IP address.
Trap Port [SNMPManagerTrapPort_x]	Defines the port number of the remote SNMP Manager. The device sends SNMP traps to this port. The valid value range is 100 to 4000. The default is 162.
Web: Trap User [SNMPManagerTrapUser]	Associates a trap user with the trap destination. This determines the trap format, authentication level, and encryption level. <ul style="list-style-type: none"> <li>v2cParams (default) = SNMPv2 user community string</li> <li>SNMPv3 user configured in 'Configuring SNMP V3 Users' on page 78</li> </ul>
Trap Enable [SNMPManagerTrapSendingEnable_x]	Activates the sending of traps to the SNMP Manager. <ul style="list-style-type: none"> <li>[0] Disable</li> <li>[1] Enable (Default)</li> </ul>

### 9.3 Configuring SNMP Trusted Managers

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



**Notes:** The SNMP Trusted Managers table can also be configured using the table ini file parameter, SNMPTrustedMgr\_x (see 'SNMP Parameters' on page 672) or CLI command, configure system > snmp > trusted-managers.

➤ **To configure SNMP Trusted Managers:**

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

**Figure 9-3: SNMP Trusted Managers**

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. Select the check box corresponding to the SNMP Trusted Manager that you want to enable and for whom you want to define an IP address.
3. Define an IP address in dotted-decimal notation.
4. Click **Submit** to apply your changes.
5. To save the changes, see 'Saving Configuration' on page 532.

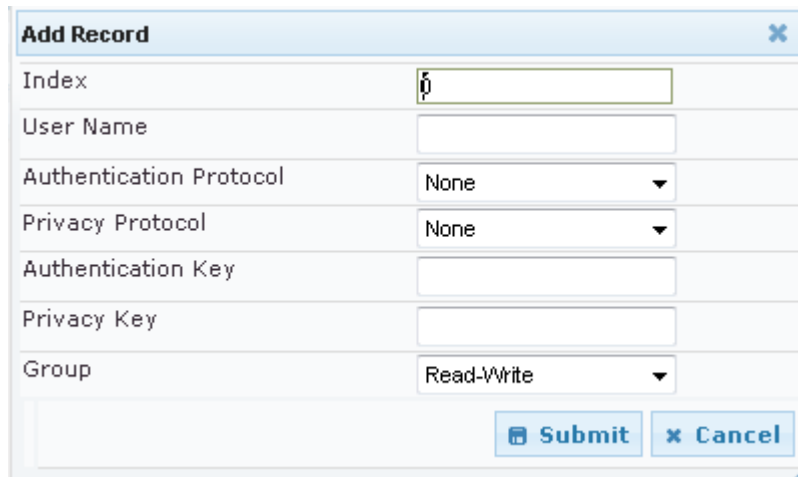
## 9.4 Configuring SNMP V3 Users

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

➤ **To configure SNMP v3 users:**

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

**Figure 9-4: SNMP V3 Setting Page - Add Record Dialog Box**



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

- Index:** A text input field with the value '1'.
- User Name:** An empty text input field.
- Authentication Protocol:** A dropdown menu with 'None' selected.
- Privacy Protocol:** A dropdown menu with 'None' selected.
- Authentication Key:** An empty text input field.
- Privacy Key:** An empty text input field.
- Group:** A dropdown menu with 'Read-Write' selected.
- Buttons:** 'Submit' and 'Cancel' buttons at the bottom right.

3. Configure the SNMP V3 Setting parameters according to the table below.
4. Click **Submit** to apply your settings.
5. To save the changes, see 'Saving Configuration' on page 532.



**Notes:**

- If you delete a user that is associated with a trap destination (in 'Configuring SNMP Trap Destinations' on page 76), the configured trap destination becomes disabled and the trap user reverts to default (i.e., SNMPv2).
- The SNMP v3 Users table can also be configured using the table ini file parameter, SNMPUsers (see 'SNMP Parameters' on page 672) or CLI command, configure system > snmp v3-users.

## SNMP V3 Users Parameters

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

## Reader's Notes

## 10 EMS-Based Management

AudioCodes Element Management System (EMS) is an advanced solution for standards-based management of MSBRs within VoP networks, covering all areas vital for the efficient operation, administration, management and provisioning (OAM&P) of AudioCodes' families of MSBRs. The EMS enables Network Equipment Providers (NEPs) and System Integrators (SIs) the ability to offer customers rapid time-to-market and inclusive, cost-effective management of next-generation networks. The standards-compliant EMS uses distributed SNMP-based management software, optimized to support day-to-day Network Operation Center (NOC) activities, offering a feature-rich management framework. It supports fault management, configuration and security.



**Note:** For more information on using the EMS tool, refer to the *EMS User's Manual* and *EMS Server IOM Manual*.

## Reader's Notes

# 11 TR-069 CWMP Based Management

The device supports TR-069 CPE WAN Management Protocol (CWMP) based management, which is used for remote management of CPE devices. This allows the device to be configured and monitored from a management application running on a remote Auto-Configuration Server (ACS).

## 11.1 TR-069

TR-069 (Technical Report 069) is a specification published by Broadband Forum ([www.broadband-forum.org](http://www.broadband-forum.org)) entitled CPE WAN management protocol (CWMP). It defines an application layer protocol for remote management of end-user devices.

TR-069 uses a bi-directional SOAP/HTTP protocol for communication between the customer premises equipment (CPE) and the Auto Configuration Servers (ACS). The TR-069 connection to the ACS can be done on the LAN or WAN interface.

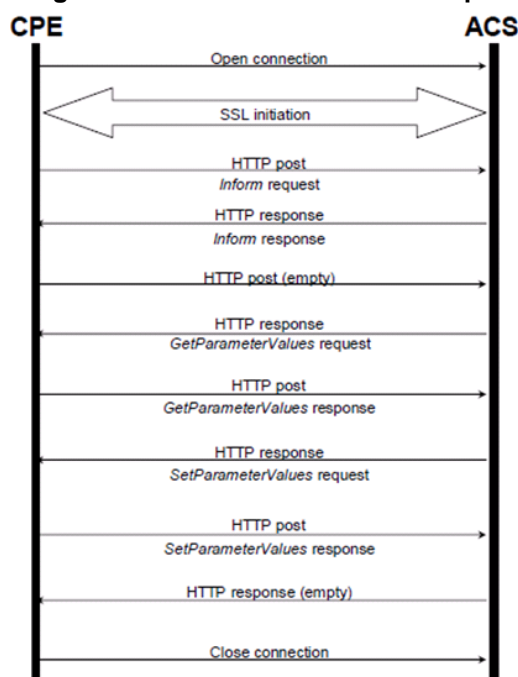
The protocol stack looks as follows:

**TR-069 Protocol Stack**

CPE/ACS Management Application
RPC Methods
SOAP
HTTP
SSL/TLS
TCP/IP

Communication is typically established by the CPE; hence, messages from CPE to ACS are typically carried in HTTP requests, and messages from ACS to CPE in HTTP responses.

**Figure 11-1: TR-069 Session Example**

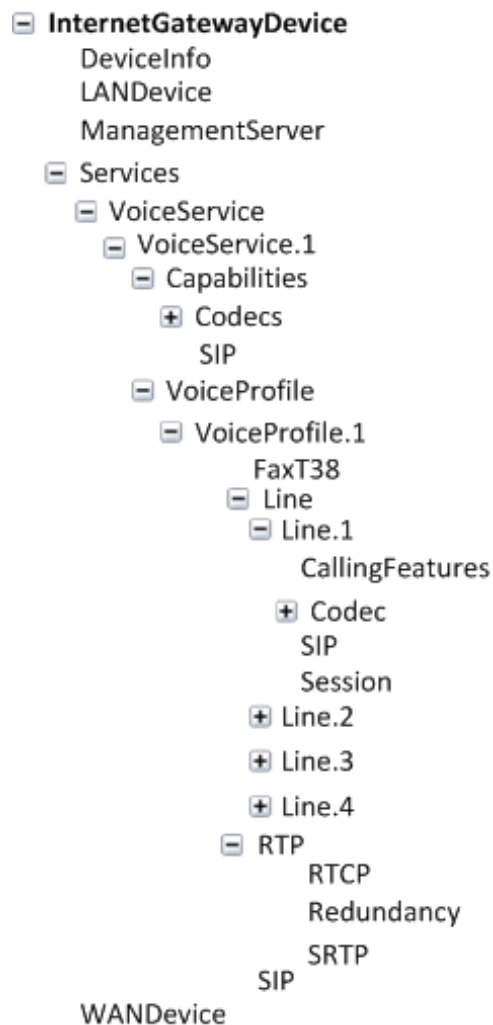


Communication between ACS and CPE is defined via Remote Procedure Call (RPC) methods. TR-069 defines a generic mechanism by which an ACS can read or write parameters to configure a CPE and monitor CPE status and statistics. It also defines the mechanism for file transfer and firmware/software management. However, it does not define individual parameters; these are defined in separate documents, as described below.

Some of the RPC methods are Configuration File Download, Firmware upgrade, Get Parameter Value, Set Parameter Value, Reboot, and the upload and download files.

TR-106 defines the “data model” template for TR-069 enabled devices. The Data Model consists of objects and parameters hierarchically organized in a tree with a single Root Object, typically named *Device*. Arrays of objects are supported by appending a numeric index to the object name (e.g. ABCService.1 in the example below); such objects are called “multi-instance objects”.

**Figure 11-2: TR-069 Model Data Example**



Below is a list of some of the TR-069 methods:

■ CPE Methods:

- GetRPCMethods: Used by the CPE or ACS to discover the set of methods supported by the Server or CPE it is in communication with.
- SetParameterValues: Used by the ACS to modify the value of CPE parameter(s).
- GetParameterValues: Used by the ACS to obtain the value of CPE parameter(s).
- GetParameterNames: Used by the ACS to discover the parameters accessible on a particular CPE.

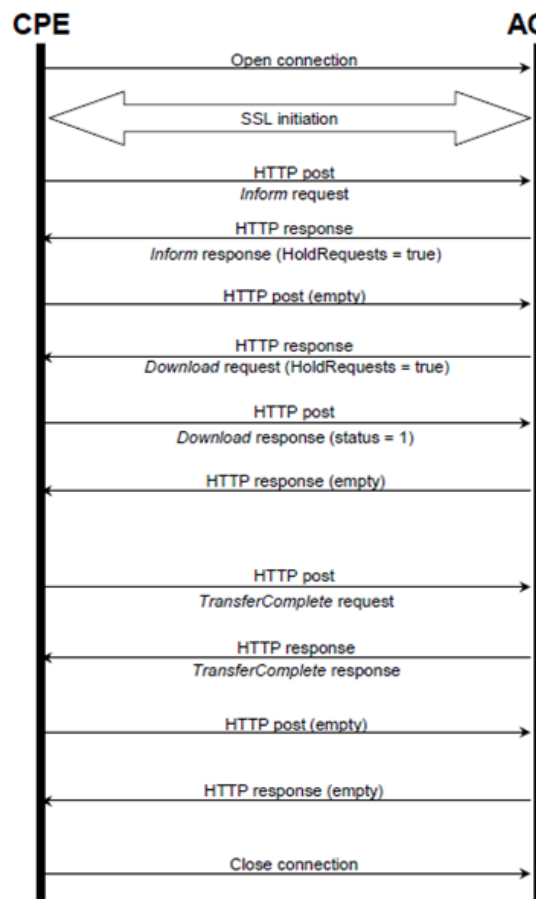


- **SetParameterAttributes:** Used by the ACS to modify attributes associated with CPE parameter(s).
- **GetParameterAttributes:** Used by the ACS to read the attributes associated with CPE parameter(s).
- **AddObject:** Used by the ACS to create a new instance of a multi-instance object—a collection of parameters and/or other objects for which multiple instances are defined.
- **DeleteObject:** Removes a particular instance of an object.
- **Download:** Used by the ACS to cause the CPE to download the following file(s) from a designated location:
  - ◆ **Firmware Upgrade Image (File Type = 1)** - cmp file.
  - ◆ **Vendor Configuration File (File Type = 3)** - output of `show running-config` CLI command, which includes Data and Voice configuration.

The CPE responds to the Download method, indicating successful or unsuccessful completion via one of the following:

- ◆ A **DownloadResponse** with the **Status** argument set to zero (indicating success), or a fault response to the Download request (indicating failure).
- ◆ A **TransferComplete** message sent later in the same session as the Download request (indicating either success or failure). In this case, the **Status** argument in the corresponding **DownloadResponse** has a value of one.
- ◆ A **TransferComplete** message sent in a subsequent session (indicating success or failure). In this case, the **Status** argument in the corresponding **DownloadResponse** has a value of one.

**Figure 11-3: Download Method Execution Example**



- Upload: Used by the ACS to cause the CPE to upload (to the ACS) the following files to a designated location:
  - ◆ Vendor Configuration File (File Type = 1 or 3): Output of `show running-config` CLI command, which includes Data and Voice configuration. For File Type 3 (where index is included – see below) only one instance of the file is supported.
  - ◆ Vendor Log File (File Type = 2 or 4): “Aggregated” log file. For File Type 2, the last file is supported. For File Type 4 (where index is included – see below), multiple files is supported.

The CPE responds to the Upload method, indicating successful or unsuccessful completion via the UploadResponse or TransferComplete method.

For a complete description of the Upload method, refer to TR-069 Amendment 3 section A.4.1.5.

- Reboot: Reboots the CPE. The CPE sends the method response and completes the remainder of the session prior to rebooting.
- X\_0090F8\_CommandResponse: Runs CLI commands.

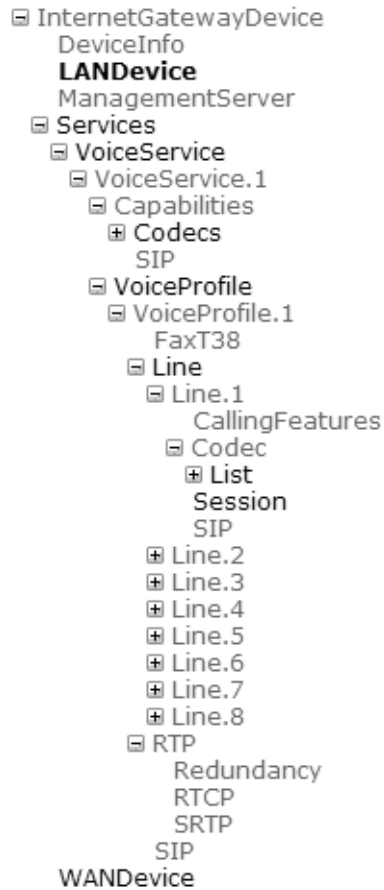
■ ACS Methods:

- Inform: A CPE must call this method to initiate a transaction sequence whenever a connection to an ACS is established.
- TransferComplete: Informs the ACS of the completion (either successful or unsuccessful) of a file transfer initiated by an earlier Download or Upload method call.

## 11.2 TR-104

The device supports TR-104 for configuration. This support is for the SIP (VoIP) application layer and applies to FXS interfaces (lines) only. TR-104 defines a "data model" template for TR-069 enabled devices. The "data model" that is applicable to the AudioCodes device is defined in the DSL Forum TR-104 – "DSLHome™ Provisioning Parameters for VoIP CPE" at <http://www.broadband-forum.org/technical/download/TR-104.pdf>.

The hierarchical tree structure of the supported TR-104 objects is shown below:

**Figure 11-4: Hierarchical Tree Structure of TR-104 Objects**

- InternetGatewayDevice.Services.VoiceService: Top-level object.
- InternetGatewayDevice.Services.VoiceService.1.Capabilities: (Read-Only) Displays the overall capabilities of the device.
  - InternetGatewayDevice.Services.VoiceService.1.Capabilities.Codecs: (Read-Only) Lists supported codecs (according to devices installed Software Feature Key).
  - InternetGatewayDevice.Services.VoiceService.1.Capabilities.SIP: (Read-Only) Displays various SIP settings such as SIP transport type.
- InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1: Corresponds to one or more FXS lines that share the same basic configuration:
  - InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.FaxT38: Configures fax T.38 relay.
  - InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line: Corresponds to an FXS line (as configured in the Trunk Group table). It enables and configures each FXS line (number).
    - ◆ InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.{i}.Code c.List.{i}: Configures voice coder used by specific FXS line.
    - ◆ InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.{i}.Callin gFeatures: Configures voice parameters per FXS line such as caller ID.
    - ◆ InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.Line.{i}.SIP: Configures username/password per FXS line. AudioCodes maps this object to the corresponding entry in the Authentication table

- InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.SIP: Configures SIP parameters specific to the UA such as Proxy server.
- InternetGatewayDevice.Services.VoiceService.1.VoiceProfile.1.RTP: Configures various RTP parameters for the FXS lines such as RTCP and SRTP.

## 11.3 Configuring TR-069

The CWMP/TR-069 Settings page is used to enable and configure TR-069.



**Notes:** For a description of the TR-069 parameters, see 'TR-069 Parameters' on page 675.

### ➤ To configure TR-069:

1. Open the CWMP/TR-069 Settings page (**Configuration** tab > **System** menu > **Management** submenu > **CWMP**).

**Figure 11-5: CWMP/TR-069 Settings Page**

▼ TR069	
TR069	Enable
Interface Name	WAN Ethernet
Protocol	HTTP
Port	82
URL	http://10.31.4.115:82/tr069/
▼ ACS	
URL	http://10.37.5.5:8080/dps-basic/TR069/
User Name	tr069
Password	tr069
▼ CPE	
User Name	dps
Password	dps
Inform Interval	20
▼ ACS Connection Status	
Session with ACS ended successfully.	

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 12 INI File-Based Management

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

**Notes:**

- For a list and description of the *ini* file parameters, see 'Configuration Parameters Reference' on page 661.
- To restore the device to default settings using the *ini* file, see 'Restoring Factory Defaults' on page 561.

### 12.1 INI File Format

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

- Individual parameters - see 'Configuring Individual ini File Parameters' on page 89
- Table parameters - see 'Configuring Table ini File Parameters' on page 89

#### 12.1.1 Configuring Individual ini File Parameters

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

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

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

For general *ini* file formatting rules, see 'General ini File Formatting Rules' on page 91.

#### 12.1.2 Configuring Table ini File Parameters

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

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

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

configured.

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

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

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

The table ini file parameter formatting rules are listed below:

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

For general *ini* file formatting rules, see 'General ini File Formatting Rules' on page 91.

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

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

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



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

### 12.1.3 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.

## 12.2 Loading an ini File

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

- Web interface, using any of the following pages:
  - Configuration File - see 'Backing Up and Loading Configuration File' on page [558](#)
  - Load Auxiliary Files - see 'Loading Auxiliary Files' on page [535](#)

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

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


**Notes:**

- For a list and description of the *ini* file parameters, see 'Configuration Parameters Reference' on page 661.
- Some parameters are configurable only through the *ini* file (and not the Web interface).
- To restore the device to default settings using the *ini* file, see 'Restoring Factory Defaults' on page 561.

## 12.3 Modifying an ini File

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

➤ **To modify an *ini* file:**

1. Save the device's configuration as an *ini* file on your computer, using the Web interface (see 'Loading an ini File' on page 91).
2. Open the *ini* file using a text file editor such as Notepad, and then modify the *ini* file parameters as required.
3. Save the modified *ini* file, and then close the file.
4. Load the modified *ini* file to the device (see 'Loading an ini File' on page 91).



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

## 12.4 Secured Encoded ini File

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


**Notes:**

- The procedure for loading an encoded *ini* file is identical to the procedure for loading an unencoded *ini* file (see 'Loading an ini File' on page 91).
- If you download from the device (to a folder on your computer) an *ini* file that was loaded encoded to the device, the file is saved as a regular *ini* file (i.e., unencoded).



# Part III

## General System Settings



## 13 Configuring Certificates

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



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

## 13.1 Replacing the Device's Certificate

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

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

1. Your network administrator should allocate a unique DNS name for the device (e.g., dns\_name.corp.customer.com). This DNS name is used to access the device and therefore, must be listed in the server certificate.
2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' parameter (HTTPSOnly) to **HTTP and HTTPS** (see 'Configuring Web Security Settings' on page 65). This ensures that you have a method for accessing the device in case the new certificate does not work. Restore the previous setting after testing the configuration.
3. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**).
4. Under the **Certificate Signing Request** group, do the following:
  - a. In the 'Subject Name [CN]' field, enter the DNS name.
  - b. Fill in the rest of the request fields according to your security provider's instructions.
  - c. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

### Figure 13-1: Certificate Signing Request Group

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

Create CSR

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

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCAR8CAQAwdjESMBAGA1UEAxMJJYXVkaW8uYy29tMRUwEwYDVQLEwIXzWFk
cXVhenRlcnMxMjEjAQBgNVBAoTCUNvenBvcmlF0ZTEVMBMGA1UEBxMUMG91Z2hrZWVw
c2llMREwDwYDVQZIEWhOZXcgWW9ayazELMAkGA1UEBHMVVMWgZ8wDQYJKoZIhVcn
AQEBBgQdgY0AMIGJAoGBAPHPf2t4OLy3FRk5Bw7Fl2FWCXQ7nvuocHtu7Nns071M
xl7Of8YoL63eeIK2eDo8nm6rJO677z/AHWJmF65pAK1CboIFgQZN30g6+5JAmJAA
1LNUnogjEsK7CF32uvolH//gFkhy5z1eNvObI+25Fn38aJzEXc8DkGwz19rRoQRZ
AgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQDihdqbci1zkHdLFr+5BRuSkYgUXBM6
q7FGjFXAfZk1MmgnBMc/MYfSGTBawrQF7p6dNJ60DivmuCPf6Gz5m2uqC6LqoIi
nLnQpVcmdbva/B1QyEpPbQhZqpULJ8CseSrrY3ru23AzeDUBvYyh090IKrBp//+3
ZvnZze5m5CBSLg==
-----END CERTIFICATE REQUEST-----

```

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

```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEw
JGUjETMBEGA1UEChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBT
ZXJ2ZXVvMB4XDTE4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1
UEBhMCRLlxEzARBgNVBAoTCkNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9z
dGUxGzU2VydMlVlcjCCASEwDQYJKoZIhvcNAQEBBQADggEEOADCCAQkCggEAPqd4Mz
iR4spWldGRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWUL
f7v7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMyb
FkzaeGrvFm4k3lRefiXDmuOe+FhJgHYeZYHf44LvPRPwhSrzi9+Ag3o8pWDguJ
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 (see 'Saving Configuration' on page 532); the Web interface uses the provided certificate.
9. Open the Certificates page again and verify that under the **Certificate information** group (at the top of the page), the 'Private key' read-only field displays "OK"; otherwise, consult your security administrator:

**Figure 13-2: Private key "OK" in Certificate Information Group**

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

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

#### Notes:

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



## 13.2 Loading a Private Key

The device is shipped with a self-generated random private key, which cannot be extracted from the device. However, some security administrators require that the private key be generated externally at a secure facility and then loaded to the device through configuration. Since private keys are sensitive security parameters, take precautions to

load them over a physically-secure connection such as a back-to-back Ethernet cable connected directly to the managing computer.

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

1. Your security administrator should provide you with a private key in either textual PEM (PKCS #7) or PFX (PKCS #12) format. The file may be encrypted with a short pass-phrase, which should be provided by your security administrator.
2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' field (HTTPSOnly) to **HTTP and HTTPS** (see 'Configuring Web Security Settings' on page 65). This ensures that you have a method for accessing the device in case the new configuration does not work. Restore the previous setting after testing the configuration.
3. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**) and scroll down to the **Upload certificate files from your computer** group.

**Figure 13-3: Upload Certificate Files from your Computer Group**

4. Fill in the 'Private key pass-phrase' field, if required.
5. Click the **Browse** button corresponding to the 'Send Private Key' field, navigate to the key file, and then click **Send File**.
6. If the security administrator has provided you with a device certificate file, load it using the 'Send Device Certificate' field.
7. After the files successfully load to the device, save the configuration with a device reset (see 'Saving Configuration' on page 532); the Web interface uses the new configuration.
8. Open the Certificates page again, and verify that under the **Certificate information** group (at the top of the page) the 'Private key' read-only field displays "OK"; otherwise, consult your security administrator.
9. If the device was originally operating in HTTPS mode and you disabled it in Step 2, then enable it by setting the 'Secured Web Connection (HTTPS)' field to **HTTPS Only**.

## 13.3 Mutual TLS Authentication

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

Since X.509 certificates have an expiration date and time, the device must be configured to use NTP (see 'Simple Network Time Protocol Support' on page 101) to obtain the current date and time. Without the correct date and time, client certificates cannot work.

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

1. Set the 'Secured Web Connection (HTTPS)' field to **HTTPS Only** (see 'Configuring Web Security Settings' on page 65) to ensure you have a method for accessing the device in case the client certificate does not work. Restore the previous setting after testing the configuration.
2. Open the Certificates page (see 'Replacing the Device's Certificate' on page 95).
3. In the **Upload certificate files from your computer** group, click the **Browse** button corresponding to the 'Send Trusted Root Certificate Store ...' field, navigate to the file, and then click **Send File**.
4. When the operation is complete, set the 'Requires Client Certificates for HTTPS connection' field to **Enable** (see 'Configuring Web Security Settings' on page 65).
5. Save the configuration with a device reset (see 'Saving Configuration' on page 532).

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

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



#### Notes:

- The process of installing a client certificate on your PC is beyond the scope of this document. For more information, refer to your operating system documentation, and/or consult your security administrator.
- The root certificate can also be loaded via the Automatic Update facility, using the HTTPSRootFileName *ini* file parameter.
- You can enable the device to check whether a peer's certificate has been revoked by an Online Certificate Status Protocol (OCSP) server (see Configuring Certificate Revocation Checking (OCSP) on page 99).

## 13.4 Self-Signed Certificates

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

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

1. Before you begin, ensure the following:
  - You have a unique DNS name for the device (e.g., dns\_name.corp.customer.com). This name is used to access the device and should therefore, be listed in the server certificate.
  - No traffic is running on the device. The certificate generation process is disruptive to traffic and should be executed during maintenance time.
2. Open the Certificates page (see 'Replacing the Device's Certificate' on page 95).
3. In the 'Subject Name **[CN]**' field, enter the fully-qualified DNS name (FQDN) as the certificate subject, select the desired private key size (in bits), and then click **Generate self-signed**; after a few seconds, a message appears displaying the new subject name.
4. Save the configuration with a device reset (see 'Saving Configuration' on page 532) for the new certificate to take effect.

## 13.5 Configuring Certificate Revocation Checking (OCSP)

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

➤ **To configure OCSP:**

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

**Figure 13-4: OCSP Parameters**

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

2. Configure the OCSP parameters as required. For a description of these parameters, see OCSP Parameters on page 693.
3. Click **Submit**.



**Notes:**

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

## 13.6 TLS Server Certificate Expiry Check

The device can periodically check the validation date of the installed TLS server certificate. This periodic check interval is user-defined. In addition, within a user-defined number of days before the installed TLS server certificate expires, the device can be configured to

send the SNMP trap, acCertificateExpiryNotification to notify of the impending certificate expiration.

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

1. Open the Certificates page (see 'Replacing the Device's Certificate' on page 95).
2. In the 'TLS Expiry Check Start' field, enter the number of days before the installed TLS server certificate is to expire at which the device must send a trap to notify of this.

**Figure 13-5: TLS Expiry Settings Group**

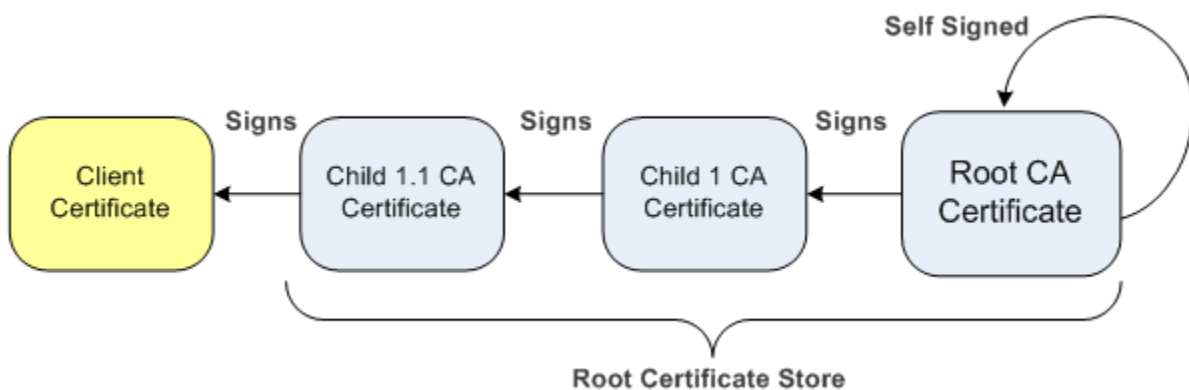
TLS Expiry Settings	
TLS Expiry Check Start (days)	<input type="text" value="60"/>
TLS Expiry Check Period (days)	<input type="text" value="7"/>
<input type="button" value="Submit TLS Expiry Settings"/>	

3. 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.
4. Click the **Submit TLS Expiry Settings** button.

## 13.7 Loading Certificate Chain for Trusted Root

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

**Figure 13-6: Certificate Chain Hierarchy**



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



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



## 14 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.

### 14.1 Configuring Date and Time Manually

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

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

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

**Figure 14-1: Regional Settings Page**

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

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



**Notes:**

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

### 14.2 Automatic Date and Time through SNTP Server

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

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

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

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

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

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

The procedure below describes how to configure SNTP.

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

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

**Figure 14-2: SNTP Configuration in Application Settings Page**

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

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

2. Configure the NTP parameters:
  - 'NTP Server DN/IP' (NTPServerIP) - defines the IP address or FQDN of the NTP server.
  - 'NTP UTC Offset' (NTPServerUTCOffset) - defines the time offset in relation to the UTC. For example, if your region is 2 hours ahead of the UTC, enter "2".
  - 'NTP Updated Interval' (NTPUpdateInterval) - defines the period after which the date and time of the device is updated.
  - 'NTP Secondary Server IP' (NTPSecondaryServerIP) - defines the secondary NTP server.
3. Configure daylight saving, if required:
  - 'Day Light Saving Time' (DayLightSavingTimeEnable) - enables daylight saving time.
  - 'DST Mode' - Determines the range type for configuring the start and end date for daylight saving:
    - ◆ **Day of Year:** The range is configured by date of month, for example, from January 4 to August 31.
    - ◆ **Day of month:** The range is configured by day of month, for example, from the second Sunday of May January to the last Sunday of August.
  - 'Start Time' (DayLightSavingTimeStart) and 'End Time' (DayLightSavingTimeEnd) - defines the period for which daylight saving time is relevant.
  - 'Offset' (DayLightSavingTimeOffset) - defines the offset in minutes to add to the time for daylight saving. For example, if your region has daylight saving of one hour, the time received from the NTP server is 11:00, and the UTC offset for your region is +2 (i.e., 13:00), you need to enter "60" to change the local time to 14:00.
4. Verify that the device is set to the correct date and time. You can do this by viewing the date and time in the Regional Settings page, as described in 'Configuring Date and Time Manually' on page 101.

## 15 Configuring Power over Ethernet

The device supports Power over Ethernet (PoE) according to the IEEE 802.3af-2003 standards, providing power on the Ethernet lines through all the LAN ports. The ports can transfer electrical power, along with the usual data, over the Ethernet cable to connected equipment (e.g., IP phones) that are capable of receiving PoE.

The LAN ports automatically detect the presence of IEEE 802.3 compliant equipment. Upon plugging in a PoE client to one of the ports, the device also automatically detects the class to which the client belongs and consequently, the maximum power allowed:

- IEEE 802.3af-2003: The device can supply up to 15.4W per port, and a total budget of 50W or 120W (depending on model) for all ports:
  - Class 0: configurable, up to 15.4W
  - Class 1: up to 4W
  - Class 2: up to 7W
  - Class 3: up to 15.4W

PoE is supplied on Pins 4,5: (+), pins 7,8: (-).

You can enable PoE per port and set the maximum port power consumption (up to 15.4W) when the plugged-in client is detected as Class 0. If the plugged-in client is detected as Class 0, the device saves the user-defined wattage from the total wattage budget (i.e., 15.4W). If the plugged-in client is detected as Class 1, Class 2, or Class 3, the device saves 4W, 7W, or 15.4W respectively from the total wattage budget. If the power budget has been exhausted and a new client is plugged in, power is unavailable to this client. You can also enable Class 4 PoE per port.



### Notes:

- PoE is a customer ordered feature.
- Upon device startup, PoE is enabled on all LAN ports.
- The power is always taken off the total budget according to the class detected, regardless of what is actually consumed per port.
- To view allocated power per port and various PoE allocation information, see 'Viewing Ethernet Port Information' on page [577](#).
- You can also configure PoE, using the ini file parameter POETable, or CLI command, **configure system/poe**.

The procedure below describes how to configure PoE through the Web interface.

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

1. Open the Power Over Ethernet Settings page (**Configuration** tab > **System** menu > **Power over Ethernet Settings**).

**Figure 15-1: Power Over Ethernet Settings Page**

Index	Port Enable	Max Power
1	<input checked="" type="radio"/> Enable	15400
2	<input type="radio"/> Enable	15400
3	<input type="radio"/> Enable	15400
4	<input type="radio"/> Enable	15400
5	<input type="radio"/> Enable	15400
6	<input type="radio"/> Enable	15400
7	<input type="radio"/> Enable	15400
8	<input type="radio"/> Enable	15400
9	<input type="radio"/> Enable	15400
10	<input type="radio"/> Enable	15400
11	<input type="radio"/> Enable	15400
12	<input type="radio"/> Enable	15400

2. Select the 'Index' radio button corresponding to the required LAN port.
3. Click the **Edit** button.
4. From the 'Port Enable' drop-down list, select whether you want to enable or disable PoE.
5. In the 'Max Power' field, enter the required maximum power consumption for the port.
6. Click **Apply**.

# Part IV

## General VoIP Configuration



# 16 Network

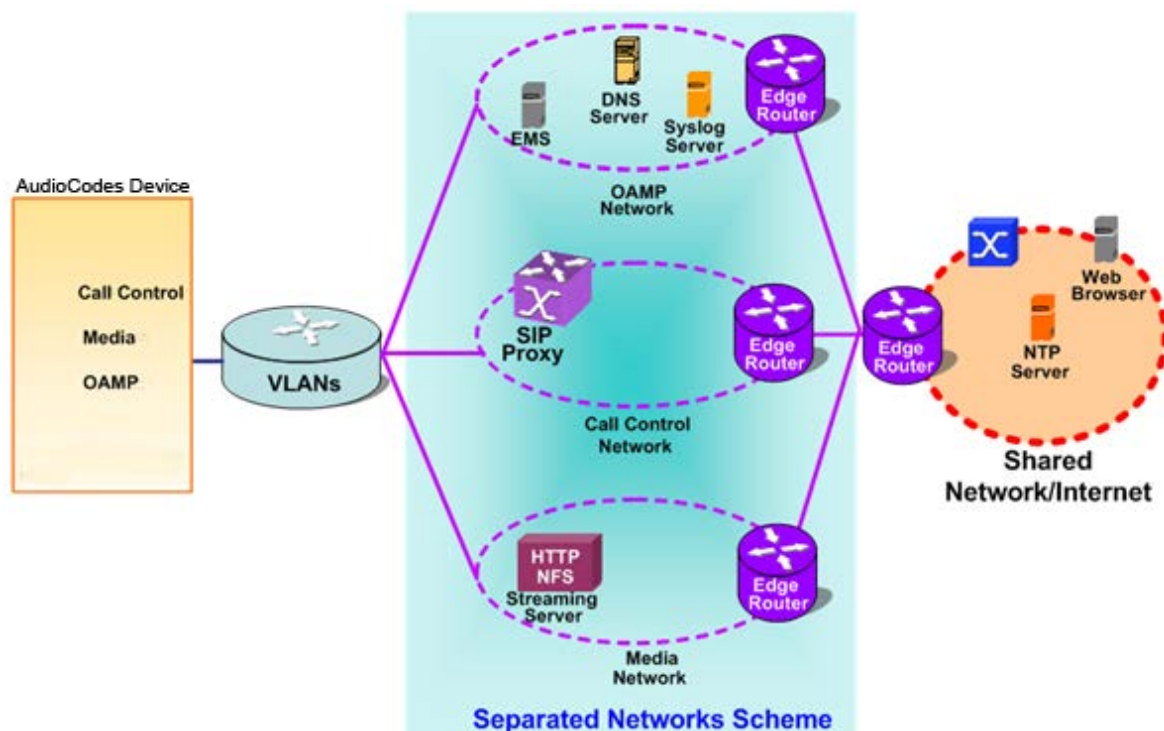
This section describes the network-related configuration.

## 16.1 Configuring IP Network Interfaces

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

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

**Figure 16-1: Multiple Network Interfaces**



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

- Application type allowed on the interface:
  - Control - call control signaling traffic (i.e., SIP)
  - Media - RTP traffic
  - Operations, Administration, Maintenance and Provisioning (OAMP) - management (such as Web- and SNMP-based management)
- IP address and subnet mask represented by prefix length
- VLAN ID
- Default Gateway - traffic from this interface destined to a subnet that does not meet any of the routing rules, local or static routes, are forwarded to this gateway
- Primary and secondary DNS IP address (optional)

You can configure up to 12 interfaces, consisting of up to 11 Control and Media interfaces and 1 OAMP interface.

The default VoIP interface is as follows:

- Application type: OAMP + Media + Control
- IP address: 192.168.0.2 with prefix length 24 (i.e., subnet mask 255.255.255.0)
- Default gateway: 192.168.0.1
- Name: "Voice"
- VLAN ID: 1

Complementing this network configuration is the On-Board Ethernet Switch configuration. This enables you to configure the VLAN IDs accessible through each physical port, as well as the Native VLAN ID of each physical port. Layer3 (DiffServ) and Layer 2 (VLAN priority) Quality of Service parameters are also configurable. For configuring Quality of Service (QoS), see 'Configuring the QoS Settings' on page 118.

Complementing the Multiple Interface table is the IP Routing table, which allows you to define VoIP network static routing rules for non-local hosts/subnets. For more information, see 'Configuring the IP Routing Table' on page 115.



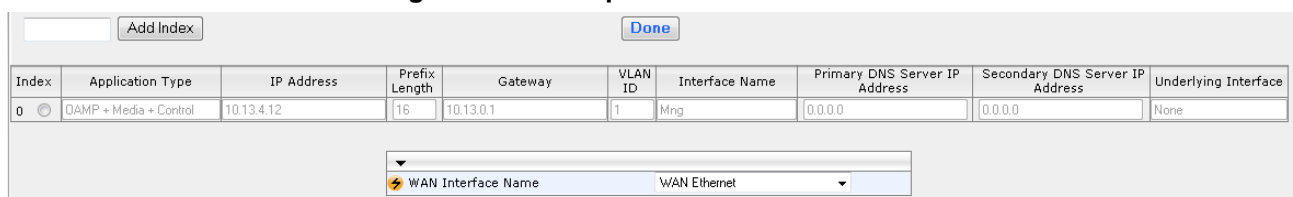
#### Notes:

- When using data-routing functionality, the network interfaces for the data-router are configured using the Data Settings menu (see Data Router Configuration on page 525).
- When operating with both voice and data-routing functionalities, it is recommended to define the default gateway IP address for the VoIP network interfaces in the same subnet and with the same VLAN ID as the IP address defined in the data-routing configuration section.
- To configure firewall rules (access list) for allowing or blocking packets received from specific IP network interfaces, see 'Configuring Firewall Settings' on page 131.
- IPv6 is currently not supported (even though it may appear in the Web interface).
- The Multiple Interface table can also be configured using the table ini file parameter, InterfaceTable (see 'Networking Parameters' on page 661) or CLI command, configure voip/interface network-if.

#### ➤ To configure VoIP network interfaces:

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

**Figure 16-2: Multiple Interface Table**



Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Interface
0	OAMP + Media + Control	10.13.4.12	16	10.13.0.1	1	Ming	0.0.0.0	0.0.0.0	None

2. In the 'Add Index' field, enter the desired index number for the new interface, and then click **Add Index**; the index row is added to the table.
3. Configure the interface according to the table below.
4. Click the **Apply** button; the interface is added to the table and the **Done** button appears.
5. Click **Done** to validate the interface. If the interface is not valid (e.g., if it overlaps with



another interface in the table or if it does not adhere to the other rules as summarized in 'Multiple Interface Table Configuration Summary and Guidelines' on page 111), a warning message is displayed.

6. Save the changes to flash memory and reset the device (see 'Saving Configuration' on page 532).

#### Multiple Interface Table Parameters Description

Parameter	Description
<b>Table parameters</b>	
Index CLI: network-if <b>[InterfaceTable_Index]</b>	Table index row of the interface. The range is 0 to 11.
Web: Application Type EMS: Application Types CLI: application-type <b>[InterfaceTable_ApplicationTypes]</b>	Defines the applications allowed on the interface. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> OAMP = Operations, Administration, Maintenance and Provisioning (OAMP) applications (e.g., Web, Telnet, SSH, and SNMP).</li> <li>▪ <b>[1]</b> Media = Media (i.e., RTP streams of voice).</li> <li>▪ <b>[2]</b> Control = Call Control applications (e.g., SIP).</li> <li>▪ <b>[3]</b> OAMP + Media = OAMP and Media applications.</li> <li>▪ <b>[4]</b> OAMP + Control = OAMP and Call Control applications.</li> <li>▪ <b>[5]</b> Media + Control = Media and Call Control applications.</li> <li>▪ <b>[6]</b> OAMP + Media + Control = All application types are allowed on the interface.</li> </ul> <b>Note:</b> For valid configuration, see 'Multiple Interface Table Configuration Rules' on page 111.
Web/EMS: IP Address CLI: ip-address <b>[InterfaceTable_IPAddress]</b>	Defines the IPv4 IP address in dotted-decimal notation. <b>Note:</b> You can configure overlapping IP addresses for multiple control and media interfaces.
Web/EMS: Prefix Length CLI: prefix-length <b>[InterfaceTable_PrefixLength]</b>	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 variable-length subnet masking technique to allow allocation on arbitrary-length prefixes.  The prefix length for IPv4 can range from 0 to 30. <b>Note:</b> For valid configuration, see 'Multiple Interface Table Configuration Rules' on page 111.
Web/EMS: Gateway CLI: gateway	Defines the IP address of the default gateway for the interface. When traffic is sent from this interface to an unknown destination (i.e., not in the

Parameter	Description
<b>[InterfaceTable_Gateway]</b>	<p>same subnet and not defined for any static routing rule), it is forwarded to this default gateway.</p> <p><b>Notes:</b> For valid configuration, see 'Multiple Interface Table Configuration Rules' on page 111.</p>
Web/EMS: VLAN ID CLI: vlan-id <b>[InterfaceTable_VlanID]</b>	<p>Defines a VLAN ID for the interface.</p> <p><b>Note:</b> For valid configuration, see 'Multiple Interface Table Configuration Rules' on page 111.</p>
Web/EMS: Interface Name CLI: name <b>[InterfaceTable_InterfaceName]</b>	<p>Defines a name for this interface. This name is used in various configuration tables to associate this network interface with other configuration entities such as Media Realms. It is also displayed in management interfaces (Web, CLI, and SNMP) for clarity where it has no functional use.</p> <p>The valid value is a string of up to 16 characters.</p> <p><b>Note:</b> For valid configuration, see 'Multiple Interface Table Configuration Rules' on page 111.</p>
Web/EMS: Primary DNS Server IP address CLI: primary-dns <b>[InterfaceTable_PrimaryDNSServerIPAddress]</b>	<p>(Optional) Defines the primary DNS server's IP address (in dotted-decimal notation), which is used for translating domain names into IP addresses for the interface.</p> <p>By default, no IP address is defined.</p>
Web/EMS: Secondary DNS Server IP address CLI: secondary-dns <b>[InterfaceTable_SecondaryDNSServerIPAddress]</b>	<p>(Optional) Defines the secondary DNS server's IP address (in dotted-decimal notation), which is used for translating domain names into IP addresses for the interface.</p> <p>By default, no IP address is defined.</p>
<b>[WanInterfaceName]</b>	<p>Assigns a WAN interface to the VoIP traffic (i.e., SIP signaling and media / RTP interfaces). The available WAN interface options depends on the hardware configuration (e.g., Ethernet, T1, or SHDSL) and/or whether VLANs are defined for the WAN interface. If VLANs are configured, for example, for the Ethernet WAN interface, then you can select the WAN VLAN on which you want to run these SIP signaling and/or media interfaces.</p> <p>The WAN interface can be assigned to SIP signaling and media interfaces in the SIP Interface table (see Configuring SIP Interface Table on page 201) and Media Realm table (see Configuring Media Realms on page 168), where the WAN interface is denoted as "WAN".</p> <p>Once this association is set, VoIP traffic is sent via the WAN and incoming traffic is identified as coming from the WAN. The device also automatically configures the required port forwarding and static NAT rules.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>If you do not assign the WAN interface to SIP and media interfaces, then the WAN interface may not be used for VoIP traffic. In such scenarios, the VoIP traffic can be sent and received within the LAN, or sent to the WAN via a third-party LAN router. If a third-party router is used as the interface to the WAN, then you need to define NAT rules (using the NATTranslation parameter) to translate the VoIP LAN IP</li> </ul>

Parameter	Description
	<p>addresses (defined in the Multiple Interface table and associated with SIP and media interfaces) into global, public IP addresses.</p> <ul style="list-style-type: none"> <li>This parameter is applicable only if the data-routing functionality is supported (i.e., relevant Software License Key is installed on the device).</li> </ul>

### 16.1.1 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.

### 16.1.2 Multiple Interface Table Configuration Rules

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

- Multiple Control and Media interfaces can be configured with overlapping IP addresses and subnets.
- The prefix length replaces the dotted-decimal subnet mask presentation and must have a value of 0-30 for IPv4 addresses.
- Only one OAMP interface must be configured and this must be an IPv4 address. This OAMP interface can be combined with Media and Control.
- At least one Control interface must be configured with an IPv4 address.
- At least one Media interface must be configured with an IPv4 address.
- 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 combined OAMP-Media interface with an IPv4 address
    - ◆ One or more combined Media-Control interfaces with IPv4 addresses.
- Each network interface can be configured with a Default Gateway. The address of the Default Gateway must be in the same subnet as the associated interface. Additional static routing rules can be configured in the IP Routing table.
- The interface name must be configured (mandatory) and unique for each interface, and can include up to 16 characters.
- For IPv4 addresses, the 'Interface Mode' column must be set to IPv4 Manual (numeric value 10).
- For network configuration to take effect, you must save the configuration to the device's flash memory (burn) with a device reset.


**Notes:**

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

### 16.1.3 Troubleshooting the Multiple Interface Table

If any of the Multiple Interface table guidelines are violated, the device falls back to a "safe mode" configuration, working temporarily with IP address 192.168.0.2. For more information on validation failures, consult the Syslog messages.

Validation failures may be caused by one of the following:

- One of the Application Types (OAMP, Control, or Media) are missing in the IPv4 interfaces.
- There are too many interfaces for Application Type, OAMP. There is only one interface defined, but the 'Application Types' column is not set to **OAMP + Media + Control** (numeric value 6).
- An IPv4 interface was defined with 'Interface Type' other than **IPv4 Manual** (10).
- Two interfaces have the same VLAN ID value.
- Two interfaces have the same name.

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

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

### 16.1.4 Networking Configuration Examples

This section provides configuration examples of networking interfaces.

#### 16.1.4.1 One VoIP Interface for All Applications

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

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

**Example of Single VoIP Interface in Multiple Interface Table**

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

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

**Example of IP Routing Table**

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

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

### 16.1.4.2 VoIP Interface per Application Type

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

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

**Example of VoIP Interfaces per Application Type in Multiple Interface Table**

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

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

**Example IP Routing Table**

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

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

### 16.1.4.3 VoIP Interfaces for Combined Application Types

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

- One interface for the OAMP application.
- Interfaces for Call Control and Media applications.

1. **Multiple Interface table:**

### Example of VoIP Interfaces of Combined Application Types in Multiple Interface Table

Index	Application Type		IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP		192.168.0.2	16	192.168.0.1	1	Mgmt
1	Media & Control		200.200.85.14	24	200.200.85.1	201	MediaCntrl1
2	Media & Control		200.200.86.14	24	200.200.86.1	202	MediaCntrl2

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

### Example of IP Routing Table

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

3. The NTP application is configured (using the ini file) to serve as OAMP applications:

```
EnableNTPasOAM = 1
```

### 16.1.4.4 VoIP Interfaces with Multiple Default Gateways

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

### Configured Default Gateway Example

Index	Applica tion Type		IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP		192.168.0.2	16	192.168.0.1	100	Mgmt
1	Media & Control		200.200.85.14	24	200.200.85.1	200	CntrlMedia

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

### Separate Routing Table Example

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

## 16.2 Configuring the IP Routing Table

The IP Routing Table page allows you to define up to 30 static IP routing rules for the device. These rules can be associated with a network interface (defined in the Multiple Interface table) and therefore, the routing decision is based on the source subnet/VLAN. If not associated with an IP interface, the static IP rule is based on destination IP address. Traffic destined to the subnet specified in the routing rule is re-directed to the defined gateway, reachable through the specified interface.

➤ **To configure static IP routing:**

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

**Figure 16-3: IP Routing Table Page**

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

**Delete Selected Entries**

Add a new table entry				
Destination IP Address	Prefix Length	Gateway IP Address	Metric	Interface Name
	16		1	

**Add New Entry**

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

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



**Notes:**

- You can delete only inactive routing rules.
- The IP Routing table can also be configured using the table ini file parameter, StaticRouteTable or the CLI command, configure voip/routing static.

### IP Routing Table Description

Parameter	Description
Destination IP Address CLI: 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 CLI: 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, 16 is synonymous with subnet 255.255.0.0.
The address of the host/network you want to reach is determined by an AND operation that is applied to the fields 'Destination IP Address' and 'Prefix Length'. For example, to reach the network 10.8.x.x, enter 10.8.0.0 in the 'Destination IP Address' field and 16 in the 'Prefix Length'. As a result of the AND operation, the value of the last two octets in the 'Destination IP Address' field is ignored. To reach a specific host, enter its IP address in the 'Destination IP Address' field and 32 in the 'Prefix Length' field.	
Gateway IP Address CLI: gateway [StaticRouteTable_Gateway]	Defines the IP address of the router (next hop) used for traffic destined to the subnet/host as defined in the 'Destination IP Address' / 'Prefix Length' field. <b>Note:</b> The Gateway address must be in the same subnet as the IP address of the interface over which you configure this static routing rule.
Metric	Defines the number of hops needed to reach the specified destination. <b>Note:</b> The recommended value for this parameter is 1. This parameter must be set to a number greater than 0 for the routing rule to be valid. Routing entries with Hop Count equals 0 are local routes set automatically by the device.
Interface Name CLI: interface-name [StaticRouteTable_InterfaceName]	Assigns a network interface through which the 'Gateway IP Address' is reached. This is the string value as configured for the network interface in the 'Interface Name' field of the Multiple Interface table (see 'Configuring IP Network Interfaces' on page 107). <b>Note:</b> The IP address of the 'Gateway IP Address' field must be in the same subnet as this interface's IP address.
Status	Read-only field displaying the status of the static IP route: <ul style="list-style-type: none"> <li>"Active" - routing rule is used by the device.</li> <li>"Inactive" - routing rule is not applied. When the destination IP address is not on the same segment with the next hop or the interface does not exist, the route state changes to "Inactive".</li> </ul>



## 16.2.1 Interface Column

This example describes the configuration of static IP routing rules.

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

**Configured Network Interfaces in Multiple Interface Table**

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

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

**Configured Static IP Routing Rules in IP Routing Table**

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

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

## 16.2.2 Routing Table Configuration Summary and Guidelines

The Routing table configurations must adhere to the following rules:

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

## 16.2.3 Troubleshooting the Routing Table

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

configure a routing rule, the device sends a notification message to the Syslog server reporting the problem.

Common routing rule configuration errors may include the following:

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



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

## 16.3 Configuring Quality of Service

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

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

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

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

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

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

**Traffic/Network Types and Priority**

Application	Traffic / Network Types	Class-of-Service (Priority)
Debugging interface	Management	Bronze
Telnet	Management	Bronze
DHCP	Management	Network
Web server (HTTP)	Management	Bronze
SNMP GET/SET	Management	Bronze
Web server (HTTPS)	Management	Bronze
RTP traffic	Media	Premium media

Application	Traffic / Network Types	Class-of-Service (Priority)
RTCP traffic	Media	Premium media
T.38 traffic	Media	Premium media
SIP	Control	Premium control
SIP over TLS (SIPS)	Control	Premium control
Syslog	Management	Bronze
SNMP Traps	Management	Bronze
DNS client	Varies according to DNS settings: <ul style="list-style-type: none"> <li>OAMP</li> <li>Control</li> </ul>	Depends on traffic type: <ul style="list-style-type: none"> <li>Control: Premium Control</li> <li>Management: Bronze</li> </ul>
NTP	Varies according to the interface type associated with NTP (see 'Assigning NTP Services to Application Types' on page 111): <ul style="list-style-type: none"> <li>OAMP</li> <li>Control</li> </ul>	Depends on traffic type: <ul style="list-style-type: none"> <li>Control: Premium control</li> <li>Management: Bronze</li> </ul>

**Notes:**

- For the QoS settings to take effect, a device reset is required.
- You can also configure the DiffServ table using the table ini file parameter DiffServToVlanPriority or CLI command, configure voip > qos vlan-mapping.

➤ **To configure QoS:**

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

**Figure 16-4: DiffServ Table Page**

Index	Differentiated Services	VLAN Priority
1	6	1

▼ Differentiated Services

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

- Configure DiffServ to VLAN priority mapping (Layer-2 QoS):
  - Enter an index entry, and then click Add.
  - In the 'Differentiated Services' field, enter the DiffServ value (0-63) and its corresponding VLAN priority level (0-7).
  - Click Submit.

3. Configure the desired DiffServ (Layer-3 QoS) values for the following traffic classes:
  - Media Premium QoS: this affects Media RTP packets sent by the VoIP towards the LAN.
  - Control Premium QoS: this affects Control Protocol (SIP) packets sent by the VoIP towards the LAN.
  - Gold QoS: this affects HTTP Streaming packets sent by the VoIP towards the LAN.
  - Bronze QoS: this affects OAMP packets sent by the VoIP towards the LAN.
4. Click **Submit** to apply your changes.
5. Save the changes to flash memory and reset the device (see 'Saving Configuration' on page 532).

## 16.4 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 120
- Internal SRV table - see 'Configuring the Internal SRV Table' on page 121

### 16.4.1 Configuring the Internal DNS Table

The Internal DNS Table page, similar to a DNS resolution, translates up to 20 host (domain) names into IP addresses. This functionality can be used when a domain name (FQDN) is configured as an IP destination for Tel-to-IP or IP-to-IP routing in the Outbound IP Routing Table or SBC IP-to-IP Routing table. Up to four different IP addresses can be assigned to the same host name. This is typically needed for alternative Tel-to-IP call routing.



#### Notes:

- The IP addresses can be configured as IPv4 and/or IPv6 addresses.
- The device initially attempts to resolve a domain name using the Internal DNS table. If the domain name isn't listed in the table, the device performs a DNS resolution using an external DNS server for the related IP network interface, configured in the Multiple Interface table (see 'Configuring IP Network Interfaces' on page 107).
- You can also configure the DNS table using the table ini file parameter, DNS2IP (see 'DNS Parameters' on page 665) or CLI command, `configure voip > control-network dns dns-to-ip`.

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

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

**Figure 16-5: Internal DNS Table - Add Record Dialog Box**

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

**Internal DNS Table Parameter Description**

Parameter	Description
Domain Name CLI: 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 CLI: first-ip-address [Dns2Ip_FirstIpAddress]	Defines the first IP address (in dotted-decimal format notation) to which the host name is translated.
Second IP Address CLI: 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 CLI: third-ip-address [Dns2Ip_ThirdIpAddress]	Defines the third IP address (in dotted-decimal format notation) to which the host name is translated.
Fourth IP Address CLI: fourth-ip-address [Dns2Ip_FourthIpAddress]	Defines the fourth IP address (in dotted-decimal format notation) to which the host name is translated.

## 16.4.2 Configuring the Internal SRV Table

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



**Notes:**

- If the Internal SRV table is configured, the device initially attempts to resolve a domain name using this table. If the domain name isn't found, the device performs a Service Record (SRV) resolution using an external DNS server configured in the Multiple Interface table (see 'Configuring IP Network Interfaces' on page 107).
- The Internal SRV table can also be configured using the table ini file parameter, SRV2IP (see 'DNS Parameters' on page 665) or CLI command, configure voip > control-network dns srv2ip.

➤ **To configure the Internal SRV table:**

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

**Figure 16-6: Internal SRV Table Page**

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

**Internal SRV Table Parameter Description**

Parameter	Description
Domain Name CLI: domain-name [Srv2lp_InternalDomain]	Defines the host name to be translated. The valid value is a string of up to 31 characters.

Parameter	Description
Transport Type CLI: transport-type [Srv2lp_TransportType]	Defines the transport type. <ul style="list-style-type: none"> <li>▪ [0] UDP (default)</li> <li>▪ [1] TCP</li> <li>▪ [2] TLS</li> </ul>
DNS Name (1-3) CLI: 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.
Priority (1-3) CLI: priority-1 2 3 [Srv2lp_Priority1/2/3]	Defines the priority of the target host. A lower value means that it is more preferred.
Weight (1-3) CLI: weight-1 2 3 [Srv2lp_Weight1/2/3]	Defines a relative weight for records with the same priority.
Port (1-3) CLI: port-1 2 3 [Srv2lp_Port1/2/3]	Defines the TCP or UDP port on which the service is to be found.

## 16.5 Configuring NFS Settings

Network File System (NFS) enables the device to access a remote server's shared files and directories and to handle them as if they're located locally. The device can use NFS to load *cmp*, *ini*, and auxiliary files through the Automatic Update mechanism (see 'Automatic Updated' on page 561).

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

### ➤ To add remote NFS file systems:


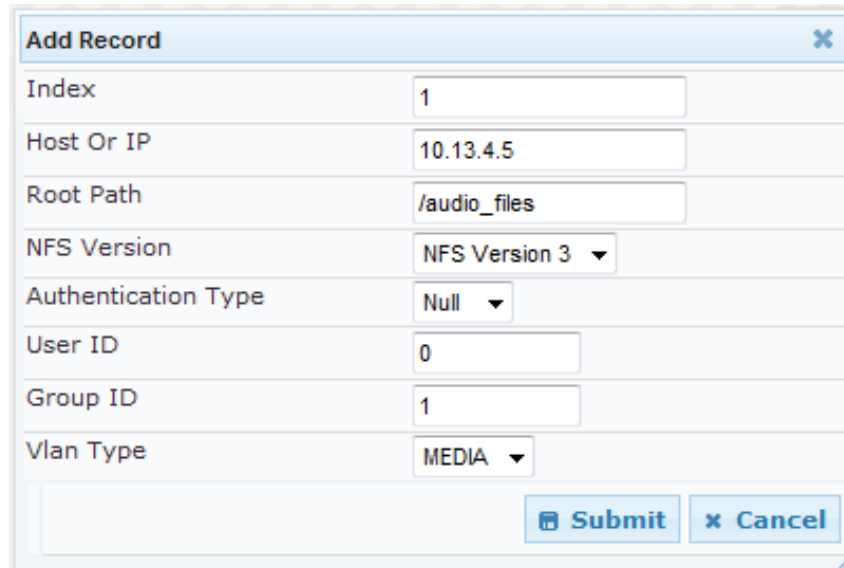
1. Open the Application Settings page (**Configuration** tab > **System** menu > **Application Settings**).
2. Under the 'NFS Settings' group, click the **NFS Table**  button; the NFS Table page appears.
3. Click the **Add** button; the Add Record dialog box appears:

Figure 16-7: Add Record Dialog Box for NFS



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

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

4. Configure the NFS parameters according to the table below.
5. Click the **Submit** button; the remote NFS file system is immediately applied, which can be verified by the appearance of the 'NFS mount was successful' message in the Syslog server.
6. To save the changes to flash memory, see 'Saving Configuration' on page 532.

**Notes:**

- To avoid terminating current calls, a row must not be deleted or modified while the device is currently accessing files on that remote NFS file system.
- The combination of 'Host Or IP' and 'Root Path' must be unique for each row in the table. For example, the table must include only one row with a Host/IP of 192.168.1.1 and Root Path of /audio.
- The NFS table can also be configured using the table ini file parameter NFSServers (see 'NFS Parameters' on page 664) or CLI command, configure system > nfs > servers.



**NFS Settings Parameters**

Parameter	Description
Index	The row index of the remote file system. The valid range is 1 to 16.
Host Or IP CLI: host [NFSServers_HostOrIP]	The domain name or IP address of the NFS server. If a domain name is provided, a DNS server must be configured.
Root Path CLI: root-path [NFSServers_RootPath]	Path to the root of the remote file system in the format: /[path]. For example, '/audio'.
NFS Version CLI: version [NFSServers_NfsVersion]	NFS version used to access the remote file system. <ul style="list-style-type: none"> <li>▪ [2] NFS Version 2</li> <li>▪ [3] NFS Version 3 (default)</li> </ul>



Parameter	Description
Authentication Type CLI: authentication-type [NFSServers_AuthType]	Authentication method used for accessing the remote file system. <ul style="list-style-type: none"> <li>[0] Null</li> <li>[1] Unix (default)</li> </ul>
User ID CLI: uid [NFSServers_UID]	User ID used in authentication when using Unix. The valid range is 0 to 65537. The default is 0.
Group ID CLI: gid [NFSServers_GID]	Group ID used in authentication when using Unix. The valid range is 0 to 65537. The default is 1.
VLAN Type CLI: vlan-type [NFSServers_VlanType]	The VLAN type for accessing the remote file system. <ul style="list-style-type: none"> <li>[0] OAM</li> <li>[1] MEDIA (default)</li> </ul> <p><b>Note:</b> This parameter applies only if VLANs are enabled or if Multiple IPs is configured (see 'Configuring IP Network Interfaces' on page 107).</p>

## 16.6 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.

### 16.6.1 Device Located behind NAT

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

- a. If configured, uses the single Static NAT IP address for all interfaces - see 'Configuring a Static NAT IP Address for All Interfaces' on page 126.
- b. If configured, uses the NAT Translation table which configures NAT per interface - see 'Configuring NAT Translation per IP Interface' on page 127.

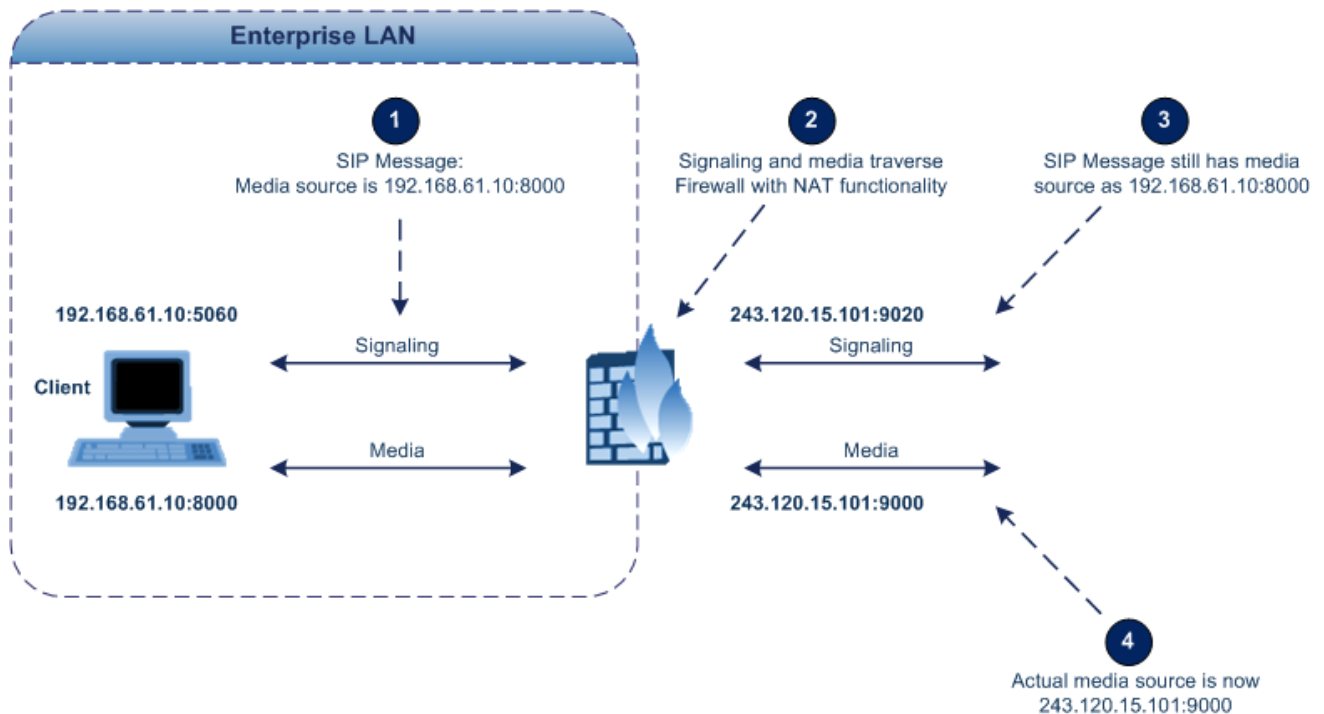
If NAT is not configured by any of the above-mentioned methods, the device sends the packet according to its IP address configured in the Multiple Interface table.



**Note:** The priority list above is applicable only to the Gateway/IP-to-IP application.

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

**Figure 16-8: Device behind NAT and NAT Issues**



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

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



**Note:** The NAT IP address can also be configured using the ini file parameter, StaticNATIP or CLI command, configure voip > sip-definition general-settings > nat-ip-addr.

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

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

**Figure 16-9: Configuring Static NAT IP Address in SIP General Parameters Page**

SIP General	
NAT IP Address	0.0.0.0

2. In the 'NAT IP Address' field, enter the NAT IP address in dotted-decimal notation.
3. Click **Submit**.
4. Save the setting to the device's flash memory with a device reset (see 'Saving Configuration' on page 532).

### 16.6.1.2 Configuring NAT Translation per IP Interface

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

If the device is configured with two network interfaces, for example, one LAN and one WAN, only one NAT rule is required and without specifying ports. This rule is defined with the network interface representing the WAN and with a public IP address.

If the device is configured with only one network interface (e.g., "Voice") and you have an SRD configured for WAN and LAN, then you need to specify ports in order to differentiate between these SRDs. In such a scenario, the device replaces the source IP address only for messages sent from the WAN SRD, not from the LAN SRD.



**Note:** The NAT Translation table can also be configured using the table ini file parameter, NATTranslation or CLI command, control-network NATTranslation.

➤ **To configure NAT translation rules:**

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

**Figure 16-10: NAT Translation Table Page**

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

3. Configure the parameters as required. For a description of the parameters, see the table below:
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 532.

### NAT Translation Table Parameters

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

## 16.6.2 Remote UA behind NAT

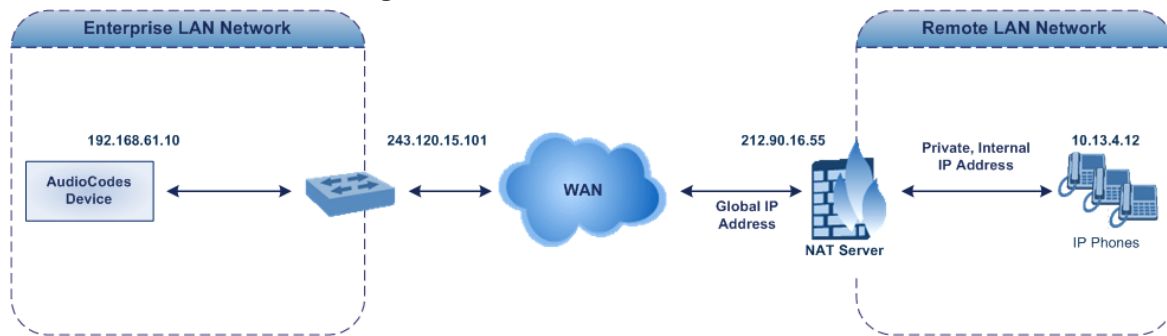
If the remote User Agent with which the device needs to communicate with is located behind NAT, the device can resolve the problem of activating the RTP/RTCP/T.38 streams to an invalid IP address / UDP port.

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

- First Incoming Packet Mechanism - see 'First Incoming Packet Mechanism' on page 129
- RTP No-Op packets according to the avt-rtp-noop draft - see 'No-Op Packets' on page 129

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

Figure 16-11: Remote UA behind NAT



### 16.6.2.1 First Incoming Packet Mechanism

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

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

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

### 16.6.2.2 No-Op Packets

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

You can control the activation of No-Op packets by using the *ini* file parameter NoOpEnable. If No-Op packet transmission is activated, you can control the time interval in which No-Op packets are sent in the case of silence (i.e., no RTP or T.38 traffic). This is done using the *ini* file parameter NoOpInterval. For a description of the RTP No-Op *ini* file parameters, see 'Networking Parameters' on page 661.

- **RTP No-Op:** The RTP No-Op support complies with IETF Internet-Draft draft-wing-avt-rtp-noop-03 ("A No-Op Payload Format for RTP"). This IETF document defines a No-Op payload format for RTP. The draft defines the RTP payload type as dynamic. You can control the payload type with which the No-Op packets are sent. This is performed using the RTPNoOpPayloadType *ini* parameter (see 'Networking Parameters' on page 661). The default payload type is 120.
- **T.38 No-Op:** T.38 No-Op packets are sent only while a T.38 session is activated. Sent packets are a duplication of the previously sent frame (including duplication of the sequence number).



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

## 16.7 Robust Receipt of Media Streams

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

The “robust-media” mechanism can be disabled by setting the InboundMediaLatchMode parameter to 0.

## 16.8 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.

# 17 Security

This section describes the VoIP security-related configuration.

## 17.1 Configuring Firewall Settings

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

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

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

### Notes:

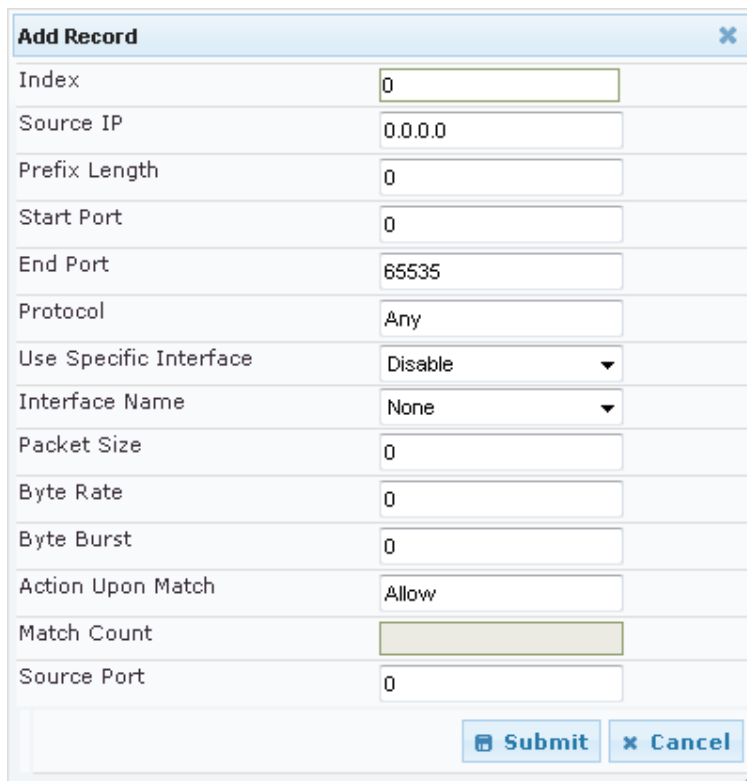
- This firewall applies to a very low-level network layer and overrides all your other security-related configuration. Thus, if you have configured higher-level security features (e.g., on the Application level), you must also configure firewall rules to permit this necessary traffic. For example, if you have configured IP addresses to access the Web and Telnet interfaces in the Web Access List (see 'Configuring Web and Telnet Access List' on page 67), you must configure a firewall rule that permits traffic from these IP addresses.
- Only Security Administrator users or Master users can configure firewall rules.
- Setting the 'Prefix Length' field to **0** means that the rule applies to **all** packets, regardless of the defined IP address in the 'Source IP' field. Therefore, it is highly recommended to set this parameter to a value other than 0.
- It is recommended to add a rule at the end of your table that blocks all traffic and to add firewall rules above it that allow required traffic (with bandwidth limitations). To block all traffic, use the following firewall rule:
  - Source IP: 0.0.0.0
  - Prefix Length: 0 (i.e., rule matches all IP addresses)
  - Start Port - End Port: 0-65535
  - Protocol: **Any**
  - Action Upon Match: **Block**
- You can also configure the firewall settings using the table ini file parameter, AccessList (see 'Security Parameters' on page 685) or the CLI command, configure voip/access-list.



➤ **To add firewall rules:**

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

**Figure 17-1: Firewall Settings Page - Add Record**



Index	0
Source IP	0.0.0.0
Prefix Length	0
Start Port	0
End Port	65535
Protocol	Any
Use Specific Interface	Disable
Interface Name	None
Packet Size	0
Byte Rate	0
Byte Burst	0
Action Upon Match	Allow
Match Count	
Source Port	0

Submit Cancel

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

The table below provides an example of configured firewall rules:

**Firewall Rule Examples**

Parameter	Value per 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.

#### Internal Firewall Parameters

Parameter	Description
Source IP CLI: 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).
Source Port CLI: 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. <b>Note:</b> When set to 0, this field is ignored and any source port matches the rule.
Prefix Length CLI: prefixLen [AccessList_PrefixLen]	<b>(Mandatory)</b> Defines the IP network mask - 32 for a single host or the appropriate value for the source IP addresses. <ul style="list-style-type: none"> <li>■ A value of 8 corresponds to IPv4 subnet class A (network mask of 255.0.0.0).</li> <li>■ A value of 16 corresponds to IPv4 subnet class B (network mask of 255.255.0.0).</li> <li>■ A value of 24 corresponds to IPv4 subnet class C (network mask of 255.255.255.0).</li> </ul> The IP address of the sender of the incoming packet is trimmed in accordance with the prefix length (in bits) and then compared to the parameter 'Source IP'. The default is 0 (i.e., applies to all packets). You <b>must</b> change this value to any of the above options. <b>Note:</b> A value of 0 applies to <b>all</b> packets, regardless of the defined IP address. Therefore, you must set this parameter to a value other than 0.
Start Port CLI: 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. <b>Note:</b> When the protocol type isn't TCP or UDP, the entire range must be provided.
End Port CLI: 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. <b>Note:</b> When the protocol type isn't TCP or UDP, the entire range must be provided.

Parameter	Description
Protocol CLI: protocol <b>[AccessList_Protocol]</b>	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. <b>Note:</b> This field also accepts the abbreviated strings 'SIP' and 'HTTP'. Specifying these strings implies selection of the TCP or UDP protocols, and the appropriate port numbers as defined on the device.
Use Specific Interface CLI: use-specific-interface <b>[AccessList_Use_Specific_Interface]</b>	Determines whether you want to apply the rule to a specific network interface defined in the Multiple Interface table (i.e., packets received from that defined in the Source IP field and received on this network interface): <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>If enabled, then in the 'Interface Name' field (described below), select the interface to which the rule is applied.</li> <li>If disabled, then the rule applies to all interfaces.</li> </ul>
Interface Name CLI: network-interface-name <b>[AccessList_Interface_ID]</b>	Defines the network interface to which you want to apply the rule. This is applicable if you enabled the 'Use Specific Interface' field. The list displays interface names as defined in the Multiple Interface table in 'Configuring IP Network Interfaces' on page 107.
Packet Size CLI: packet-size <b>[AccessList_Packet_Size]</b>	Defines the maximum allowed packet size. The valid range is 0 to 65535. <b>Note:</b> When filtering fragmented IP packets, this field relates to the overall (re-assembled) packet size, and not to the size of each fragment.
Byte Rate CLI: byte-rate <b>[AccessList_Byte_Rate]</b>	Defines the expected traffic rate (bytes per second), i.e., the allowed bandwidth for the specified protocol. In addition to this field, the 'Burst Bytes' field provides additional allowance such that momentary bursts of data may utilize more than the defined byte rate, without being interrupted.  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 CLI: byte-burst <b>[AccessList_Byte_Burst]</b>	Defines the tolerance of traffic rate limit (number of bytes). The default is 0.
Action Upon Match CLI: allow-type <b>[AccessList_Allow_Type]</b>	Defines the firewall action to be performed upon rule match. <ul style="list-style-type: none"> <li>"Allow" = (Default) Permits these packets</li> <li>"Block" = Rejects these packets</li> </ul>
Match Count <b>[AccessList_MatchCount]</b>	(Read-only) Displays the number of packets accepted or rejected by the rule.

## 17.2 Configuring General Security Settings

The General Security Settings page is used to configure various security features. For a description of the parameters appearing on this page, refer 'Configuration Parameters Reference' on page 661.

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

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

**Figure 17-2: General Security Settings Page**

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

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 532.

## 17.3 Intrusion Detection System

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

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

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

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

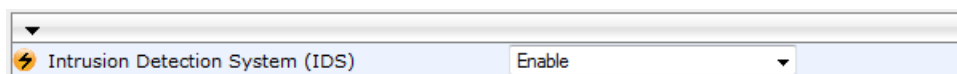
### 17.3.1 Enabling IDS

The procedure below describes how to enable IDS.

#### ➤ To enable IDS:

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

**Figure 17-3: Enabling IDS on IDS Global Parameters Page**



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

## 17.3.2 Configuring IDS Policies

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

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



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

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

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

These default policies are read-only.

➤ **To configure IDS policies:**

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

**Figure 17-4: IDS Policy Table with Default Rules**

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

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

**Figure 17-5: IDS Policy Table - Add Record**

Add Record	
Index	3
Name	SIP-Trunk
Description	for attacks from SIP Trunk
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

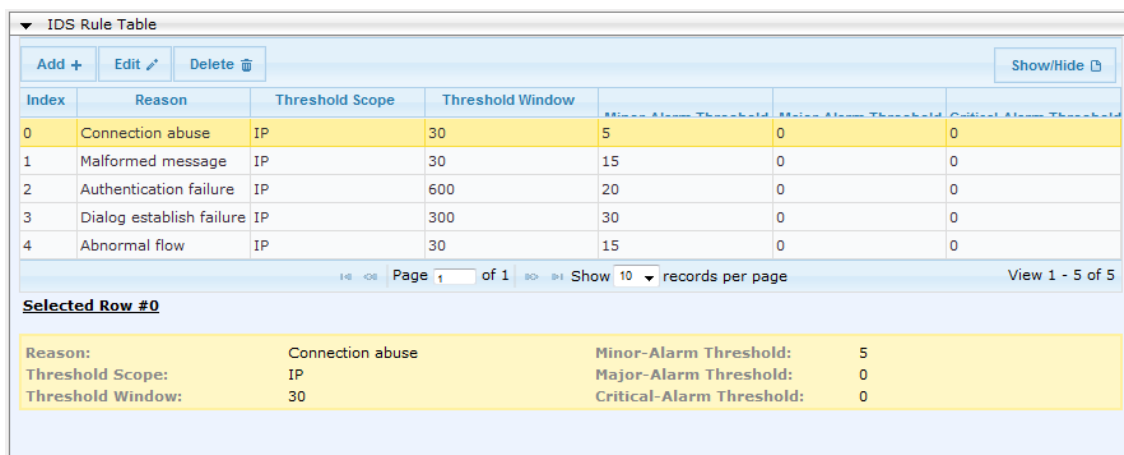
- b. Configure the parameters as described in the following table, and then click **Submit**.

### IDS Policy Table Parameters

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

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

**Figure 6: IDS Rule Table of Selected IDS Policy**



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

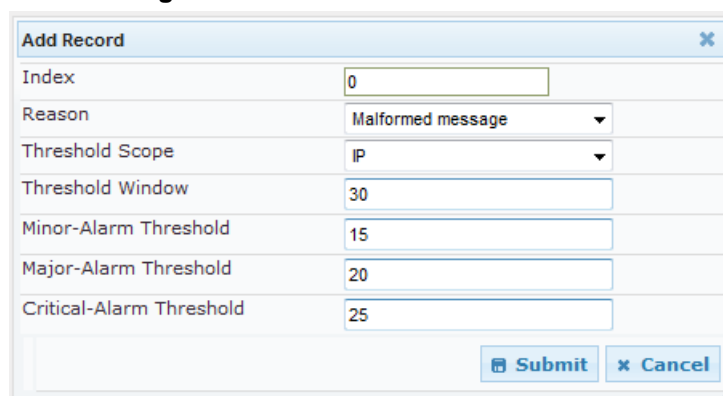
Page 1 of 1 Show 10 records per page View 1 - 5 of 5

**Selected Row #0**

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

- b. Click **Add**.

**Figure 7: IDS Rule Table - Add Record**



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

Submit Cancel

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

IDS Rule Table Parameters

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

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

### 17.3.3 Assigning IDS Policies

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

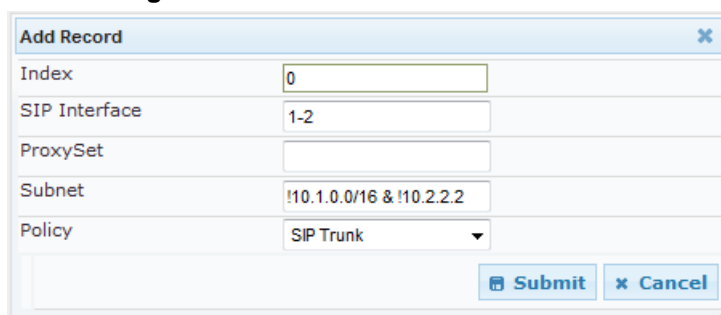
- **SIP Interface:** Detects malicious attacks (according to specified IDS Policy) on specific SIP Interface(s)
- **Proxy Sets:** Detects malicious attacks (according to specified IDS Policy) from specified Proxy Set(s)
- **Subnet addresses:** Detects malicious attacks (according to specified IDS Policy)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

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

➤ **To assign an IDS policy:**

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

**Figure 8: IDS Match Table - Add Record**



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

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



## IDS Match Table Parameters

Parameter	Description
Index CLI: sip-interface [IDSMatch_Index]	Defines the table row number for the rule.
SIP Interface CLI: 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. The entered value must be the ID of the SIP Interface. The following syntax is supported:</p> <ul style="list-style-type: none"> <li>A comma-separated list of SIP Interface IDs (e.g., 1,3,4)</li> <li>A hyphen "-" indicates a range of SIP Interfaces (e.g., 3,4-7 means IDs 3, and 4 through 7)</li> <li>A prefix of an exclamation mark "!" means negation of the set (e.g., !3,4-7 means all indexes excluding 3, and excluding 4 through 7)</li> </ul>
ProxySet CLI: 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"> <li>A comma-separated list of Proxy Set IDs (e.g., 1,3,4)</li> <li>A hyphen "-" indicates a range of Proxy Sets (e.g., 3,4-7 means IDs 3, and 4 through 7)</li> <li>A prefix of an exclamation mark "!" means negation of the set (e.g., !3,4-7 means all indexes excluding 3, and excluding 4 through 7)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Only the IP address of the Proxy Set is considered (not the port).</li> <li>If a Proxy Set has multiple IP addresses, the device considers the Proxy Set as one entity and includes all its IP addresses in the same IDS count.</li> </ul>
Subnet CLI: subnet [IDSMatch_Subnet]	<p>Defines the subnet(s) to which the IDS policy is assigned. This indicates the subnets from where the attacks are coming from. The following syntax can be used:</p> <ul style="list-style-type: none"> <li>Basic syntax is a subnet in CIDR notation (e.g., 10.1.0.0/16 means all sources with IP address in the range 10.1.0.0–10.1.255.255)</li> <li>An IP address can be specified without the prefix length to refer to the specific IP address.</li> <li>Each subnet can be negated by prefixing it with "!", which means all IP addresses outside that subnet.</li> <li>Multiple subnets can be specified by separating them with "&amp;" (and) or " " (or) operations. For example: <ul style="list-style-type: none"> <li>✓ 10.1.0.0/16   10.2.2.2: includes subnet 10.1.0.0/16 and IP address 10.2.2.2.</li> <li>✓ !10.1.0.0/16 &amp; !10.2.2.2: includes all addresses except those of subnet 10.1.0.0/16 and IP address 10.2.2.2. Note that the exclamation mark "!" appears before each subnet.</li> <li>✓ 10.1.0.0/16 &amp; !10.1.1.1: includes subnet 10.1.0.0/16, except IP address 10.1.1.1.</li> </ul> </li> </ul>
Policy CLI: policy [IDSMatch_Policy]	Selects the IDS policy, configured in 'Configuring IDS Policies' on page <a href="#">137</a> .

## 17.3.4 Viewing IDS Alarms

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

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

The SNMP alarm is cleared after a user-defined period (configured by the ini file parameter, 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 137). 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 figure below shows an example of IDS alarms in the Active Alarms table (Viewing Active Alarms), where a minor threshold alarm is cleared and replaced by a major threshold alarm:

**Figure 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

You can also view the IDS alarms in the CLI:

- To view active IDS alarms:

```
show voip security ids active-alarm all
```

- To view all IP addresses that crossed the threshold for an active IDS alarm:

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

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

**Types of Malicious Events and Syslog Text String**

Type	Description	Syslog String
<b>Connection Abuse</b>	TLS authentication failure	abuse-tls-auth-fail
<b>Malformed Messages</b>	<ul style="list-style-type: none"> <li>Message exceeds a user-defined maximum message length (50K)</li> <li>Any SIP parser error</li> <li>Message policy match</li> <li>Basic headers not present</li> <li>Content length header not present (for TCP)</li> <li>Header overflow</li> </ul>	<ul style="list-style-type: none"> <li>malformed-invalid-msg-len</li> <li>malformed-parse-error</li> <li>malformed-message-policy</li> <li>malformed-miss-header</li> <li>malformed-miss-content-len</li> <li>malformed-header-overflow</li> </ul>
<b>Authentication Failure</b>	<ul style="list-style-type: none"> <li>Local authentication ("Bad digest" errors)</li> <li>Remote authentication (SIP 401/407 is sent if original message includes authentication)</li> </ul>	<ul style="list-style-type: none"> <li>auth-establish-fail</li> <li>auth-reject-response</li> </ul>

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

## Reader's Notes

## 18 Media

This section describes the media-related configuration.

### 18.1 Configuring Voice Settings

The Voice Settings page configures various voice parameters such as voice volume, silence suppression, and DTMF transport type. For a detailed description of these parameters, see 'Configuration Parameters Reference' on page 661.

➤ **To configure the voice parameters:**

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

▼		
Voice Volume (-32 to 31 dB)	0	
Input Gain (-32 to 31 dB)	0	
Silence Suppression	Disable	▼
DTMF Transport Type	RFC2833 Relay DTMF	▼
DTMF Volume (-31 to 0 dB)	-11	
NTE Max Duration	-1	
CAS Transport Type	CASEventsOnly	▼
⚡ DTMF Generation Twist	0	
Echo Canceller	Enable	▼

2. Configure the Voice parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

#### 18.1.1 Configuring Voice Gain (Volume) Control

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

The procedure below describes how to configure gain control using the Web interface:

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

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

**Figure 18-1: Voice Volume Parameters in Voice Settings Page**

Voice Volume (-32 to 31 dB)	0
Input Gain (-32 to 31 dB)	0

2. Configure the following parameters:
  - 'Voice Volume' (*VoiceVolume*) - Defines the voice gain control (in decibels) for IP-to-Tel
  - 'Input Gain' (*InputGain*) - Defines the PCM input gain control (in decibels) for Tel-to-IP
3. Click **Submit** to apply your settings.

## 18.1.2 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 procedure below describes how to enable silence suppression using the Web interface.

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

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

**Figure 18-2: Enabling Silence Suppression in Voice Settings Page**



The screenshot shows a web interface for 'Voice Settings'. A label 'Silence Suppression' is followed by a dropdown menu currently set to 'Enable'. To the right of the dropdown is a blue circular icon with a white pencil, indicating an edit or save action.

2. Set the 'Silence Suppression' (*EnableSilenceCompression*) field to **Enable**.
3. Click **Submit** to apply your changes.

## 18.1.3 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 Canceler, 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 procedure below describes how to configure echo cancellation using the Web interface:

➤ **To configure echo cancellation using the Web interface:**

1. Configure line echo cancellation:

- a. Open the Voice Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Voice Settings**).

Echo Canceller	Enable
▼ Acoustic Echo Suppressor Settings	
⚡ Network Echo Suppressor Enable	Disable
Echo Canceller Type	Line echo canceller
Attenuaion Intensity	0
Max ERL Threshold - DB	0
Min Reference Delay x10 msec	0
Max Reference Delay x10 msec	40

- b. Set the 'Echo Canceller' field (*EnableEchoCanceller*) to **Enable**.

2. Enable acoustic echo cancellation for SBC calls:

- a. 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

- b. Open the IP Profile Settings page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** submenu > **IP Profile Settings**), and set the 'Echo Canceller' field to **Acoustic**.

- c. 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

## 18.2 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.



### Notes:

- 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 160).
- For a detailed description of the parameters appearing on this page, see 'Configuration Parameters Reference' on page 661.

### ➤ To access the fax and modem parameters:

1. Open the Fax/Modem/CID Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Fax/Modem/CID Settings**).

General Settings	
Fax Transport Mode	RelayEnable
Caller ID Transport Type	Mute
Caller ID Type	Standard Bellcore
V.21 Modem Transport Type	Disable
V.22 Modem Transport Type	Enable Bypass
V.23 Modem Transport Type	Enable Bypass
V.32 Modem Transport Type	Enable Bypass
V.34 Modem Transport Type	Enable Bypass
Fax CNG Mode	Disable
CNG Detector Mode	Disable

Fax Relay Settings	
Fax Relay Redundancy Depth	0
Fax Relay Enhanced Redundancy Depth	4
Fax Relay ECM Enable	Enable
Fax Relay Max Rate (bps)	33600bps
T38 Version	T.38 version 0

Bypass Settings	
Fax/Modem Bypass Coders Type	G711Alaw_64
Fax/Modem Bypass Packing Factor	1
Fax Bypass Output Gain	0
Modem Bypass Output Gain	0

V.150.1 Modem Relay Settings	
SSE Payload Type Rx	105
SSE Payload Type Tx	105
SSE Redundancy Depth	3
SPRT Payload Type Rx	115
SPRT Payload Type Tx	115
SPRT Transport Ch.0 Max Payload Size	140
SPRT Transport Ch.2 Max Payload Size	132
SPRT Transport Ch.2 Max Window Size	8
SPRT Transport Ch.3 Max Payload Size	140

2. Configure the parameters, as required.
3. Click **Submit** to apply your changes.



## 18.2.1 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 160): 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`).

## 18.2.2 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 149)
- G.711 Transport: switching to G.711 when fax/modem is detected (see 'G.711 Fax / Modem Transport Mode' on page 151)
- Fax fallback to G.711 if T.38 is not supported (see 'Fax Fallback' on page 151)
- Fax and modem bypass: a proprietary method that uses a high bit rate coder (see 'Fax/Modem Bypass Mode' on page 152)
- NSE Cisco's Pass-through bypass mode for fax and modem (see 'Fax / Modem NSE Mode' on page 153)
- Transparent with events: passing the fax / modem signal in the current voice coder with adaptations (see 'Fax / Modem Transparent with Events Mode' on page 154)
- Transparent: passing the fax / modem signal in the current voice coder (see 'Fax / Modem Transparent Mode' on page 154)
- RFC 2833 ANS Report upon Fax/Modem Detection (see 'RFC 2833 ANS Report upon Fax/Modem Detection' on page 155)

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

### 18.2.2.1 T.38 Fax Relay Mode

In Fax Relay mode, fax signals are transferred using the T.38 protocol. T.38 is an 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 150)
- 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 150)

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`). This 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.

### 18.2.2.1.1 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. In the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**), set the 'Fax Signaling Method' parameter to **T.38 Relay** (IsFaxUsed = 1).
2. In 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).

### 18.2.2.1.2 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. In the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**), set the 'Fax Signaling Method' parameter to **No Fax** (IsFaxUsed = 0).
2. In the Fax/Modem/CID Settings page, set the 'Fax Transport Mode' parameter to **RelayEnable** (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)

### 18.2.2.2 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  $\mu$ -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:**

- In the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**), set the 'Fax Signaling Method' parameter to **G.711 Transport** (IsFaxUsed = 2).

### 18.2.2.3 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  $\mu$ -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:**

- In the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions > General Parameters**), set the 'Fax Signaling Method' parameter to **Fax Fallback** (IsFaxUsed = 3).

#### 18.2.2.4 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. In the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions > General Parameters**), set the 'Fax Signaling Method' parameter to **No Fax** (IsFaxUsed = 0).
2. In 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) - in the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media > RTP/RTCP Settings**).
  - ModemBypassPayloadType (ini file).
  - FaxModemBypassBasicRTTPacketInterval (ini file).
  - FaxModemBypasDJBufMinDelay (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.

### 18.2.2.5 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. In the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions > General Parameters**), set the 'Fax Signaling Method' parameter to **No Fax** (IsFaxUsed = 0).
2. In 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.

### 18.2.2.6 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. In the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**), set the 'Fax Signaling Method' parameter to **No Fax** (IsFaxUsed = 0).
2. In 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).

### 18.2.2.7 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 233) 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. In the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**), set the 'Fax Signaling Method' parameter to **No Fax** (IsFaxUsed = 0).
2. In 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 table - (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders**).
    - b. 'Dynamic Jitter Buffer Optimization Factor' (DJBufOptFactor) - RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** > **RTP/RTCP Settings**).
    - c. 'Silence Suppression' (EnableSilenceCompression) - Voice Settings page (**Configuration** tab > **VoIP** menu > **Media** > **Voice Settings**).
    - d. 'Echo Canceller' (EnableEchoCanceller) - Voice Settings page.



**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 152) or Transparent with Events modes (see 'Fax / Modem Transparent with Events Mode' on page 154) for modem.

### 18.2.2.8 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. This 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. In the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**), set the 'Fax Signaling Method' parameter to **No Fax** or **Fax Fallback** (IsFaxUsed = 0 or 3).
2. In 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).

## 18.2.3 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:

- T38 Version 3 - V.34 fax relay mode
- Bypass mechanism for V.34 fax transmission (see 'Bypass Mechanism for V.34 Fax Transmission' on page 156)
- T38 Version 0 relay mode, i.e., fallback to T.38 (see 'Relay Mode for T.30 and V.34 Faxes' on page 156)

To configure whether to pass V.34 over T38 fax relay, or use Bypass over the High Bit Rate coder (e.g. PCM A-Law), use the 'V.34 Fax Transport Type' parameter (V34FaxTransportType).

You can use the 'SIP T38 Version' parameter (SIPT38Version) in the Advanced Parameters page (Configuration tab > VoIP menu > SIP Definitions > Advanced Parameters) to configure one of the following:

- Pass V.34 over T.38 fax relay using bit rates of up to 33,600 bps ('SIP T38 Version' is set to Version 3).
- Use Fax-over-T.38 fallback to T.30, using up to 14,400 bps ('SIP T38 Version' is set to Version 0).



**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**.

### 18.2.3.1 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. In 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).
2. Set the ini file parameter, V34FaxTransportType to 2 (Bypass).

#### ➤ To use bypass mode for V.34 faxes, and T.38 for T.30 faxes:

1. In the Fax/Modem/CID Settings page, do the following:
  - a. Set the 'Fax Transport Mode' parameter to **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).
2. Set the ini file parameter, V34FaxTransportType to 2 (Bypass).

### 18.2.3.2 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. In the Fax/Modem/CID Settings page, do the following:
  - a. Set the 'Fax Transport Mode' parameter to **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).
2. Set the ini file parameter, V34FaxTransportType to 1 (Relay).

➤ **To allow V.34 fax relay over T.38:**

- In the Advanced Parameters page (Configuration tab > VoIP menu > SIP Definitions > Advanced Parameters), set the 'SIP T38 Version' parameter to Version 3 (SIPT38Version = 3).

➤ **To force V.34 fax machines to use their backward compatibility with T.30 faxes and operate in the slower T.30 mode:**

- Set the 'SIP T38 Version' parameter to Version 0 (SIPT38Version = 0).

### 18.2.3.3 V.34 Fax Relay for SG3 Fax Machines

Super Group 3 (SG3) is a standard for fax machines that support speeds of up to 33.6 kbps through V.34 half duplex (HD) modulation. This procedure below describes how to configure V.34 (SG3) fax relay support based on ITU Specification T.38 version 3.

➤ **To enable support for V.34 fax relay (T.38) at SG3 speed:**

1. In the IP Profile table (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **IP Profile Settings**), configure an IP Profile with the 'Fax Signaling Method' parameter (IpProfile\_IsFaxUsed) set to **T.38 Relay**.
2. In the Coders Table (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders**), set the coder used by the device to G.729 (or any other supported codec).
3. On the Fax/Modem/CID Settings page, do the following:
  - a. Set the 'SIP T38 Version' parameter to Version 3 (SIPT38Version = 3).
  - b. Set the 'Fax Relay Max Rate' parameter (RelayMaxRate) to **33,600bps** (default).
  - c. Set the 'CNG Detector Mode' parameter (CNGDetectorMode) to **Disable** (default).
  - d. Set the 'V.21 Modem Transport Type' parameter to **Disable** (V21ModemTransportType = 0).
  - e. Set the 'V.22 Modem Transport Type' parameter to **Disable** (V22ModemTransportType = 0).
  - f. Set the 'V.23 Modem Transport Type' parameter to **Disable** (V23ModemTransportType = 0).
  - g. Set the 'V.32 Modem Transport Type' parameter to **Disable** (V32ModemTransportType = 0).
  - h. Set the 'V.34 Modem Transport Type' parameter to **Disable** (V34ModemTransportType = 0).
4. Set the ini file parameter, V34FaxTransportType to 1 (i.e., relay).
5. Set the ini file parameter, T38MaxDatagramSize to 560 (default).

6. Set the ini file parameter, CEDTransferMode to 0 (default).


**Notes:**

- The T.38 negotiation should be completed at call start according to V.152 procedure (as shown in the INVITE example below).
- T.38 mid-call Re-INVITEs are supported.
- If the remote party supports only T.38 Version 0, the device "downgrades" the T.38 Version 3 to T.38 Version 0.

For example, the device sends or receives the following INVITE message, negotiating both audio and image media:

```
INVITE sip:2001@10.8.211.250;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.6.55;branch=z9hG4bKac1938966220
Max-Forwards: 70
From: <sip:318@10.8.6.55>;tag=1c1938956155
To: <sip:2001@10.8.211.250;user=phone>
Call-ID: 193895529241200022331@10.8.6.55
CSeq: 1 INVITE
Contact: <sip:318@10.8.6.55:5060>
Supported: em,100rel,timer,replaces,path,resource-priority,sdp-
  anat
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
  SCRIBE,UPDATE
Remote-Party-ID:
<sip:318@10.8.211.250>;party=calling;privacy=off;screen=no;screen-
  ind=0;npi=1;ton=0
Remote-Party-ID: <sip:2001@10.8.211.250>;party=called;npi=1;ton=0
User-Agent: Audiocodes-Sip-Gateway-/v.6.00A.013.007
Content-Type: application/sdp
Content-Length: 433

v=0
o=AudiocodesGW 1938931006 1938930708 IN IP4 10.8.6.55
s=Phone-Call
c=IN IP4 10.8.6.55
t=0 0
m=audio 6010 RTP/AVP 18 97
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:97 telephone-event/8000
a=fmtp:97 0-15
a=ptime:20
a=sendrecv
m=image 6012 udpt1 t38
a=T38FaxVersion:3
a=T38MaxBitRate:33600
a=T38FaxMaxBuffer:1024
a=T38FaxMaxDatagram:122
a=T38FaxRateManagement:transferredTCF
a=T38FaxUdpEC:t38UDPRedundancy
```

## 18.2.4 V.150.1 Modem Relay

The device can be configured to transfer modem calls using a subset of the ITU-T V.150.1 Modem Relay protocol. The device also supports V.150.1 modem relay coder negotiation

in the initial SIP INVITE and 200 OK using the SDP body (according to the UCR-2008, Change 2 specification). This eliminates the need for sending a re-INVITE to negotiate V.150.1. The device sends an INVITE's SDP offer in a format to negotiate V.150 modem relay using the same port as RTP, as shown in the example below:

```
a=cdisc:1 audio udpsprt 114\r\n
a=cpar:a=sprtmap:114 v150mr/8000\r\n
a=cpar:a=fmtp:114
mr=1;mg=0;CDSCselect=1;mrmods=1,3;jmdelay=no;versn=1.1\r\n\
```

You can configure the payload type for the outgoing SDP offer, using the NoAudioPayloadType parameter. You can set this parameter to "NoAudio", whereby RTP is not sent and the device adds an audio media only for the Modem Relay purpose. This is also in accordance to DOD UCR 2008 specification: "The AS-SIP signaling appliance MUST advertise the "NoAudio" payload type to interoperate with a "Modem Relay-Preferred" endpoint that immediately transitions to the Modem Relay state without first transmitting voice information in the Audio state."



#### Notes:

- The V.150.1 Modem Relay feature support is a subset of the full V.150.1 protocol and is designed according to the US DOD requirement document. It therefore, cannot be used for general purposes.
- The V.150.1 Modem Relay feature is available only if the device is installed with the V.150.1 Software License Key.
- The V.150.1 feature has been tested with certain IP phones. For more details, please contact your AudioCodes sales representative.
- The V.150.1 SSE Tx payload type is according to the offered SDP of the remote side.
- The V.150.1 SPRT Rx payload type is according to the 'Payload Type' field in the Coders table.
- The V.150.1 SPRT Tx payload type is according to the remote side offered SDP.

#### ➤ To configure V.150.1 Modem relay:

1. In the Coders Table (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders**), set the coder to **V.150**.
2. On the Fax/Modem/CID Settings page, configure the V.150.1 parameters appearing under the 'V.150.1 Modem Relay Settings' group:
  - a. Set the 'SSE Payload Type Rx' parameter to the V.150.1 SSE payload type that the device uses when it offers the SDP.
  - b. Set the 'SSE Redundancy Depth' parameter to the number of sent SSE redundant packets. This parameter is important in case of network impairments.
  - c. For additional V.150.1 related parameters, see 'Fax and Modem Parameters' on page 753.

## 18.2.5 Simultaneous Negotiation of Fax (T.38) and Modem (V.150.1) Relay

The device can negotiate fax relay (T.38) and modem relay (V.150.1) sessions in the same, already established call channel. Fax relay sessions require bypass answering tone (CED) while modem relay requires RFC 2833 answering tone. As the device is not always aware at the start of the session whether the answering tone is fax or modem, it uses both

methods for CED tone transfer and sends both answering tone types. Only when the answering tone is detected, does the device send the fax or modem.

To support this functionality, you need to configure a Coders Group (in the Coders Group table - see 'Configuring Coders Groups' on page 236) that includes the T.38, V.150, and G.711/VBD coders.

## 18.2.6 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  $\mu$ -law). The selection of capabilities is performed using the coders table (see 'Configuring Coders' on page 233).

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  $\mu$ -law and G.729.

```
v=0
o=- 0 0 IN IPV4 <IPAdressA>
s=-
t=0 0
p=+1
c=IN IP4 <IPAdressA>
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. To configure T.38 mode, use the CodersGroup parameter.



**Note:** You can also configure the device to handle G.711 coders received in INVITE SDP offers as VBD coders, using the HandleG711asVBD parameter. For example, if the device is configured with G.729 and G.711 VBD coders and it receives an INVITE with an SDP offer containing G.729 and "regular" G.711 coders, it sends an SDP answer containing G.729 and G.711 VBD coders, allowing subsequent bypass (passthrough) sessions if fax / modem signals are detected during the call.

## 18.2.7 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.

## 18.3 Configuring RTP/RTCP Settings

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

### 18.3.1 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 procedure below 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 (**Configuration** tab > **VoIP** menu > **Media** submenu > **RTP/RTCP Settings**). The relevant parameters are listed under the 'General Settings' group, as shown below:

**Figure 18-3: Jitter Buffer Parameters in the RTP/RTCP Settings Page**

General Settings	
Dynamic Jitter Buffer Minimum Delay	<input type="text" value="10"/>
Dynamic Jitter Buffer Optimization Factor	<input type="text" value="10"/>

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 **Submit** to apply your settings.

## 18.3.2 Comfort Noise Generation

The device can generate artificial background noise, called *comfort* noise, in the voice channel during periods of silence (i.e. when no call party is speaking). This is useful in that it reassures the call parties that the call is still connected. The device detects silence using its Voice Activity Detection (VAD) mechanism. When the Calling Tone (CNG) is enabled and silence is detected, the device transmits Silence Identifier Descriptors (SIDs) parameters to reproduce the local background noise at the remote (receiving) side.

The Comfort Noise Generation (CNG) support also depends on the silence suppression (SCE) setting for the coder used in the voice channel. For more information, see the description of the CNG-related parameters.

The procedure below describes how to configure CNG using the Web interface.

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

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

**Figure 18-4: Comfort Noise Parameter in RTP/RTCP Settings Page**

Comfort Noise Generation Negotiation	<input type="text" value="Enable"/>
--------------------------------------	-------------------------------------

2. Set the 'Comfort Noise Generation Negotiation' parameter (ComfortNoiseNegotiation) to **Enable**.
3. Click **Submit** to apply your changes.



## 18.3.3 Dual-Tone Multi-Frequency Signaling

This section describes the configuration of Dual-Tone Multi-Frequency (DTMF) signaling.

### 18.3.3.1 Configuring DTMF Transport Types

The device supports various methods for transporting DTMF digits over the IP network to the remote endpoint. These methods and their configuration are configured in the DTMF & Dialing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **DTMF and Supplementary** > **DTMF & Dialing**):

- **Using INFO message according to Nortel IETF draft:** DTMF digits are sent to the remote side in INFO messages. To enable this mode, define the following:
  - a. Set the 'Declare RFC 2833 in SDP' parameter to **No** (RxDTMFOption = 0).
  - b. Set the '1st Tx DTMF Option' parameter to **INFO (Nortel)** (TxDTMFOption = 1).**Note:** In this mode, DTMF digits are removed from the audio stream (and the 'DTMF Transport Type' parameter is automatically set to **Mute DTMF**).
- **Using INFO message according to Cisco's mode:** DTMF digits are sent to the remote side in INFO messages. To enable this mode, define the following:
  - a. Set the 'Declare RFC 2833 in SDP' parameter to **No** (RxDTMFOption = 0).
  - b. Set the '1st Tx DTMF Option' parameter to **INFO (Cisco)** (TxDTMFOption = 3).**Note:** In this mode, DTMF digits are removed from the audio stream (and the 'DTMF Transport Type' parameter is automatically set to **Mute DTMF**).
- **Using NOTIFY messages according to IETF Internet-Draft draft-mahy-sipping-signaled-digits-01:** DTMF digits are sent to the remote side using NOTIFY messages. To enable this mode, define the following:
  - a. Set the 'Declare RFC 2833 in SDP' parameter to **No** (RxDTMFOption = 0).
  - b. Set the '1st Tx DTMF Option' parameter to **NOTIFY** (TxDTMFOption = 2).**Note:** In this mode, DTMF digits are removed from the audio stream (and the 'DTMF Transport Type' parameter is automatically set to **Mute DTMF**).
- **Using RFC 2833 relay with Payload type negotiation:** DTMF digits are sent to the remote side as part of the RTP stream according to RFC 2833. To enable this mode, define the following:
  - a. Set the 'Declare RFC 2833 in SDP' parameter to **Yes** (RxDTMFOption = 3).
  - b. Set the '1st Tx DTMF Option' parameter to **RFC 2833** (TxDTMFOption = 4).**Note:** To set the RFC 2833 payload type with a value other than its default, use the RFC2833PayloadType parameter. The device negotiates the RFC 2833 payload type using local and remote SDP and sends packets using the payload type from the received SDP. The device expects to receive RFC 2833 packets with the same payload type as configured by this parameter. If the remote side doesn't include 'telephony-event' in its SDP, the device sends DTMF digits in transparent mode (as part of the voice stream).
- **Sending DTMF digits (in RTP packets) as part of the audio stream (DTMF Relay is disabled):** This method is typically used with G.711 coders. With other low-bit rate (LBR) coders, the quality of the DTMF digits is reduced. To enable this mode, define the following:
  - a. Set the 'Declare RFC 2833 in SDP' parameter to **No** (RxDTMFOption = 0).
  - b. Set the '1st Tx DTMF Option' parameter to **Not Supported** (TxDTMFOption = 0).
  - c. Set the ini file parameter, DTMFTransportType to 2 (i.e., transparent).
- **Using INFO message according to Korea mode:** DTMF digits are sent to the remote side in INFO messages. To enable this mode, define the following:

- a. Set the 'Declare RFC 2833 in SDP' parameter to **No** (RxDTMFOption = 0).
- b. Set the '1st Tx DTMF Option' parameter to **INFO (Cisco)** (TxDTMFOption = 3).

**Note:** In this mode, DTMF digits are removed from the audio stream (and the 'DTMF Transport Type' parameter is automatically set to **Mute DTMF**).



#### Notes:

- The device is always ready to receive DTMF packets over IP in all possible transport modes: INFO messages, NOTIFY, and RFC 2833 (in proper payload type) or as part of the audio stream.
- To exclude RFC 2833 Telephony event parameter from the device's SDP, set the 'Declare RFC 2833 in SDP' parameter to **No**.

The following parameters affect the way the device handles the DTMF digits:

- TxDTMFOption, RxDTMFOption, RFC2833TxPayloadType, and RFC2833RxPayloadType
- MGCPDTMFDetectionPoint, DTMFVolume, DTMFTransportType, DTMFDigitLength, and DTMFInterDigitInterval

### 18.3.3.2 Configuring RFC 2833 Payload

The procedure below describes how to configure the RFC 2833 payload using the Web interface:

#### ➤ To configure RFC 2833 payload using the Web interface:

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

**Figure 18-5: RFC 2833 Payload Parameters in RTP/RTCP Settings Page**

RTP Redundancy Depth	0
Packing Factor	1
Basic RTP Packet Interval	Default ▼
RFC 2833 TX Payload Type	96
RFC 2833 RX Payload Type	96
RFC 2198 Payload Type	104
Fax Bypass Payload Type	102
Enable RFC 3389 CN Payload Type	Enable ▼

2. Configure the following parameters:
  - 'RTP Redundancy Depth' (RTPRedundancyDepth) - enables the device to generate RFC 2198 redundant packets.
  - 'Enable RTP Redundancy Negotiation' (EnableRTPRedundancyNegotiation) - enables the device to include the RTP redundancy dynamic payload type in the SDP, according to RFC 2198.
  - '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 **Submit** to apply your settings.



### 18.3.4 Configuring RTP Base UDP Port

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

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

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

Where the port offsets are as follows:

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

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

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

- BaseUDPPort to (BaseUDPPort + 255\*10) - for example, if the BaseUDPPort is set to 6,000, then the UDP port range is 6,000 to 8,550



#### Notes:

- The device allocates the UDP ports randomly to the channels.
- To configure the device to use the same port for both RTP and T.38 packets, set the T38UseRTPPort parameter to 1.
- If you are using Media Realms (see 'Configuring Media Realms' on page 168), the port range configured for the Media Realm must be within this range defined by the BaseUDPPort parameter.

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

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

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

**Figure 18-6: RTP Based UDP Port in RTP/RTCP Settings Page**

⚡ RTP Base UDP Port	6000
---------------------	------

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

## 18.4 Configuring IP Media Settings

This section describes the configuration of various IP media features.

### 18.4.1 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 or PSTN, 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.



**Note:** AGC is a customer ordered feature and thus, must be included in the Software License Key installed on the device.

The procedure below describes how to configure AGC using the Web interface:

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

1. Open the IPMedia Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **IPMedia Settings**). The AGC parameters are shown in the figure below:

**Figure 18-7: AGC Parameters in IPMedia Settings Page**

Enable AGC	Enable
AGC Slope	3
AGC Redirection	0
AGC Target Energy	19

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



**Note:** Below are additional AGC parameters:

- AGCMinGain - Defines the minimum gain (in dB) by the AGC when activated
- AGCMaxGain - Defines the maximum gain (in dB) by the AGC when activated.
- AGCDisableFastAdaptation - Enables the AGC Fast Adaptation mode

## 18.5 Configuring Analog Settings

The Analog Settings page allows you to configure various analog parameters. For a detailed description of the parameters appearing on this page, see 'Configuration Parameters Reference' on page 661.

This page also selects the type (USA or Europe) of FXS and/or FXO coefficient information. The FXS coefficient contains the analog telephony interface characteristics such as DC and AC impedance, feeding current, and ringing voltage.

➤ **To configure the analog parameters:**

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

**Figure 18-8: Analog Settings Page**

▼ FXS_FXO Settings	
⚡ Analog TTX Voltage Level	0.5V ▼
⚡ Analog Metering Type	12 kHz sinusoidal bursts ▼
⚡ Min. Hook-Flash Detection Period [msec]	300
Max. Hook-Flash Detection Period [msec]	700
⚡ FXS Coefficient Type	USA ▼
⚡ FXO Coefficient Type	USA ▼

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 18.6 Configuring Various Codec Attributes

The following codec attributes can be configured in the General Media Settings page:

- AMR coder:
  - 'Payload Format': Defines the AMR payload format type.
- 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.

For a detailed description of these parameters and for additional codec parameters, see 'Coder Parameters' on page 747.

➤ **To configure general media parameters:**

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

**Figure 18-9: Coder Attribute Configuration in General Media Settings Page**

▲ General Settings	
▼ SILK Coders Settings	
Silk Tx Inband FEC	Disable
Silk Max Average Bit Rate	16000
▼ AMR Bandwidth Efficient Configuration	
AMR Payload Format	Octet Aligned

2. Configure the parameters as required, and then click **Submit**.
3. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 18.7 Configuring Media Realms

The Media Realm Table page allows you to define a pool of up to 64 SIP media interfaces, termed *Media Realms*. Media Realms allow you to divide a Media-type interface, which is configured in the Multiple Interface table, into several realms, where each realm is specified by a UDP port range. You can also define the maximum number of sessions per Media Realm. Once configured, Media Realms can be assigned to IP Groups (see 'Configuring IP Groups' on page 204) or SRDs (see 'Configuring SRD Table' on page 199).

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

- Quality of Experience parameters for reporting to AudioCodes SEM server used for monitoring the quality of calls (see 'Configuring Quality of Experience Parameters per Media Realm' on page 170)
- Bandwidth management (see 'Configuring Bandwidth Management per Media Realm' on page 173)



**Notes:**

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

➤ **To define a Media Realm:**

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

**Figure 18-10: Media Realm Page - Add Record Dialog Box**

3. Configure the parameters as required. See the table below for a description of each parameter
4. Click **Submit** to apply your settings.
5. Reset the device to save the changes to flash memory (see 'Saving Configuration' on page 532).

**Media Realm Table Parameter Descriptions**

Parameter	Description
Index [CpMediaRealm_Index]	Defines the required table index number.
Media Realm Name CLI: name [CpMediaRealm_MediaRealmName]	Defines an arbitrary, identifiable name for the Media Realm. The valid value is a string of up to 40 characters. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ This parameter is mandatory.</li> <li>▪ The name assigned to the Media Realm must be unique.</li> <li>▪ This Media Realm name is used in the SRD and IP Groups table.</li> </ul>
IPv4 Interface Name CLI: ipv4 [CpMediaRealm_IPv4IF]	Assigns an IPv4 interface to the Media Realm. This is name of the interface as configured for the Interface Name field in the Multiple Interface table.
Port Range Start CLI: port-range-start [CpMediaRealm_PortRangeStart]	Defines the starting port for the range of Media interface UDP ports. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ You must either configure all media realms with port ranges or all without; not some with and some without.</li> <li>▪ The available UDP port range is calculated using the BaseUDPport parameter:</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>✓ BaseUDPport to BaseUDPport + 255*10</li> <li>▪ Port ranges over 60,000 must not be used.</li> </ul>
Number of Media Session Legs CLI: session-leg [CpMediaRealm_MediaSessionLeg]	Defines the number of media sessions associated with the range of ports. This is the number of media sessions available in the port range. For example, 100 ports correspond to 10 media sessions, since ports are allocated in chunks of 10.
Port Range End CLI: port-range-end [CpMediaRealm_PortRangeEnd]	Read-only field displaying the ending port for the range of Media interface UDP ports. This field is calculated by adding the 'Media Session Leg' field (multiplied by the port chunk size) to the 'Port Range Start' field. A value appears once a row has been successfully added to the table.
Is Default CLI: is-default [CpMediaRealm_IsDefault]	<p>Defines the Media Realm as the default Media Realm. This default Media Realm is used when no Media Realm is configured for an IP Group or SRD for a specific call.</p> <ul style="list-style-type: none"> <li>▪ [0] No (default)</li> <li>▪ [1] Yes</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter can be set to <b>Yes</b> for only <b>one</b> defined Media Realm.</li> <li>▪ If this parameter is not configured, then the first Media Realm in the table is used as the default.</li> <li>▪ If the table is not configured, then the default Media Realm includes all the configured media interfaces.</li> </ul>

## 18.7.1 Configuring Quality of Experience per Media Realm

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

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

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

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

- Packet loss
- Mean Opinion Score (MOS)
- Jitter
- Packet delay
- Residual Echo Return Loss (RERL)

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

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

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



**Notes:**

- The QoE feature is available only if the device is installed with the relevant Software License Key.
- To configure the address of the AudioCodes Session Experience Manager (SEM) server to where the device reports the QoE, see 'Configuring SEM Server for Media Quality of Experience' on page 175.
- You can also configure QoE per Media Realm using the table *ini* file parameter QOERules or CLI command, media qoe-rules.

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

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

**Figure 18-11: Quality of Experience Page - Add Record Dialog Box**

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

The figure above shows value thresholds for the MOS parameter, which are assigned using pre-configured values of the Low Sensitivity profile. In this example setting, if the MOS value changes by 0.1 (hysteresis) to 3.3 or 3.5, the device sends a report to the

SEM indicating this change. If the value changes to 3.3, it sends a yellow state (i.e., medium quality); if the value changes to 3.5, it sends a green state.

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

#### Quality of Experience Parameter Descriptions

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



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

## 18.7.2 Configuring Bandwidth Management per Media Realm

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

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

Bandwidth management includes the following bandwidth utilization states:

- Normal
- High threshold
- Critical threshold

When a transition occurs between two bandwidth threshold states, based on threshold and hysteresis values, the device executes the configured action. The transition possibilities include Normal-High threshold state changes and High-Critical threshold state changes.

Thus, up to two thresholds can be configured per Media Realm; one for each state transition.



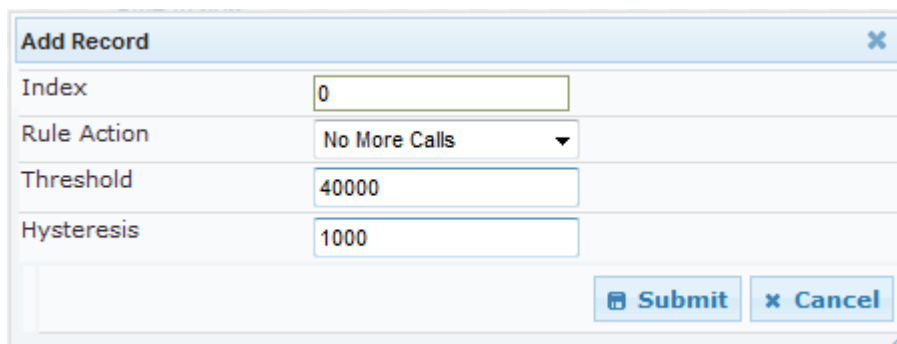
#### Notes:

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

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

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

**Figure 18-12: Bandwidth Management Page - Add record Dialog Box**



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

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

#### Bandwidth Management Parameter Descriptions

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

Parameter	Description
Threshold CLI: threshold [BWManagement_Threshold]	Defines the bandwidth threshold in bytes per second (Bps). The default is 0.
Hysteresis CLI: hysteresis [BWManagement_Hysteresis]	Defines the bandwidth fluctuation (change) from the threshold value at which the device performs the configured action. The default is 0.

## 18.8 Configuring Server for Media Quality of Experience

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



### Notes:

- To support this feature, the device must be installed with the relevant Software License Key.
- To configure the parameters to report and their thresholds per Media Realm, see 'Configuring Quality of Experience per Media Realm' on page 170.
- For information on the SEM server, refer to the *EMS User's Manual*.

### ➤ To configure QoE reporting of media:

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

Figure 18-13: Media Quality of Experience Page

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

2. Configure the parameters as required
  - 'Server Ip' (QOEServerIP) - defines the IP address of the SEM server
  - 'Port' (QOEPort) - defines the port of the SEM server
  - 'Interface Name' (QOEInterfaceName) - defines the device's IP network interface on which the SEM reports are sent
  - 'Use Mos LQ' (QOEUseMosLQ) - defines the reported MOS type (listening or conversational)
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 18.9 Configuring Media Security

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

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

- AES\_CM\_128\_HMAC\_SHA1\_32
- AES\_CM\_128\_HMAC\_SHA1\_80
- ARIA\_CM\_128\_HMAC\_SHA1\_80
- ARIA\_CM\_192\_HMAC\_SHA1\_80

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

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

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

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

Below is an example of crypto attributes usage:

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

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

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



### Notes:

- For a detailed description of the SRTP parameters, see SRTP Parameters on page 687.
- When SRTP is used, the channel capacity may be reduced.

➤ **To configure media security:**

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

**Figure 18-14: Media Security Page**

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

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## Reader's Notes

## 19 Services

This section describes configuration for various supported services.

### 19.1 Routing Based on LDAP Active Directory Queries

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

#### 19.1.1 Configuring the LDAP Server

The basic LDAP mechanism is described below:

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

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

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

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



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

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

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

The LDAP Settings page is used for configuring the LDAP server parameters. For a full description of these parameters, see 'Configuration Parameters Reference' on page [661](#).

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

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

**Figure 19-1: LDAP Settings Page**

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

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

- "Not Applicable"
  - "Connection Broken"
  - "Connecting"
  - "Connected"
2. Configure the parameters as required.
  3. Click **Submit** to apply your changes.
  4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 19.1.2 Configuring the Device's LDAP Cache

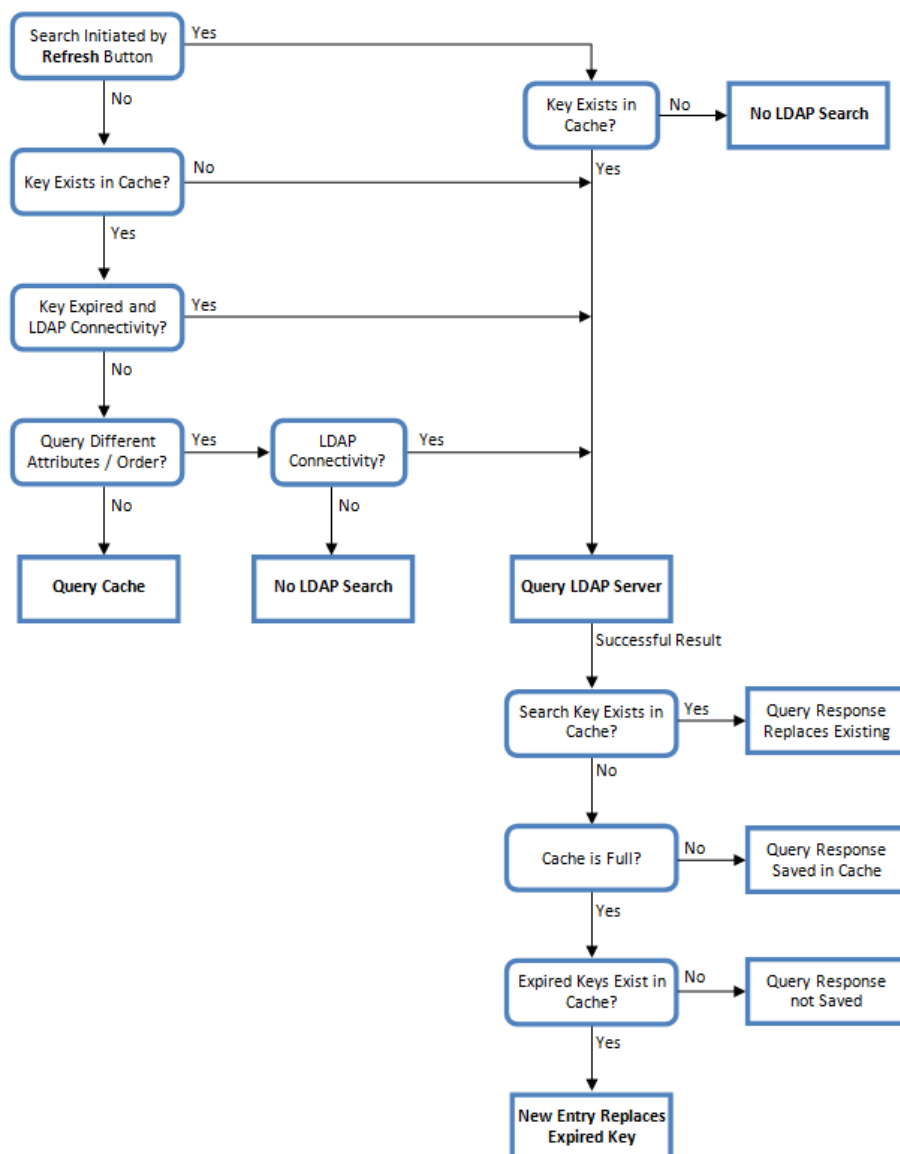
The device provides an option for storing recent LDAP queries and responses in its local cache. The cache is used for subsequent queries and/or in case of LDAP server failure. The advantage of enabling this feature includes the following:

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



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

**Figure 19-2: LDAP Query Process with Local LDAP Cache**



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



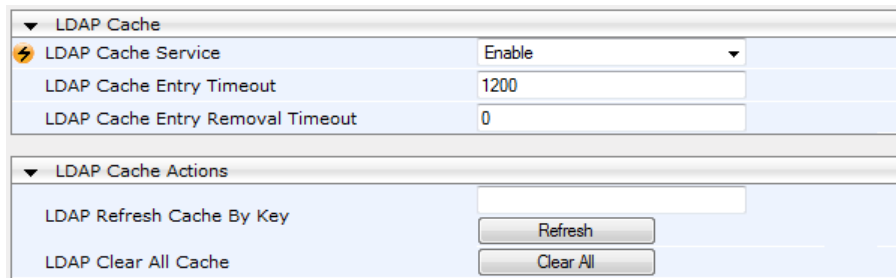
**Notes:**

- The LDAP cache parameters are available only if you have enabled the LDAP service (see 'Configuring the LDAP Server' on page 179).
- If on the first LDAP query, the result fails for at least one attribute and is successful for at least one, the partial result is cached. However, for subsequent queries, the device does not use the partially cached result, but does a new query with the LDAP server again.
- For a full description of the cache parameters, see 'Configuration Parameters Reference' on page 661.

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

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

**Figure 19-3: LDAP Settings Page - Cache Parameters**



LDAP Cache	
LDAP Cache Service	Enable
LDAP Cache Entry Timeout	1200
LDAP Cache Entry Removal Timeout	0

LDAP Cache Actions	
LDAP Refresh Cache By Key	<input type="text"/> Refresh
LDAP Clear All Cache	Clear All

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

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

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

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

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

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

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

#### 19.1.3.1 Querying the AD and Routing Priority

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

## Parameters for Configuring Query Attribute Key

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

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

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

In addition, it queries the special attribute defined in MSLDAPPrivateNumAttributeName, only if the query key (primary or secondary) is equal to its value.
5. If the query is found: The AD returns up to four attributes - Lync / OCS, PBX / IP PBX, private (only if it equals Primary or Secondary key), and mobile.
6. The device adds unique prefix keywords to the query results in order to identify the query type (i.e., IP domain). These prefixes are used as the prefix destination number value in the Outbound IP Routing table to denote the IP domains:
  - "PRIVATE" (PRIVATE:<private\_number>): used to match a routing rule based on query results of the private number (MSLDAPPrivateNumAttributeName)
  - "OCS" (OCS:<Lync\_number>): used to match a routing rule based on query results of the Lync client number (MSLDAPOCSNumAttributeName)

- "PBX" (PBX:<PBX\_number>): used to match a routing rule based on query results of the PBX / IP PBX number (MSLDAPPBXNumAttributeName)
- "MOBILE" (MOBILE:<mobile\_number>): used to match a routing rule based on query results of the mobile number (MSLDAPMobileNumAttributeName)
- "LDAP\_ERR": used to match a routing rule based on a failed query result when no attribute is found in the AD



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

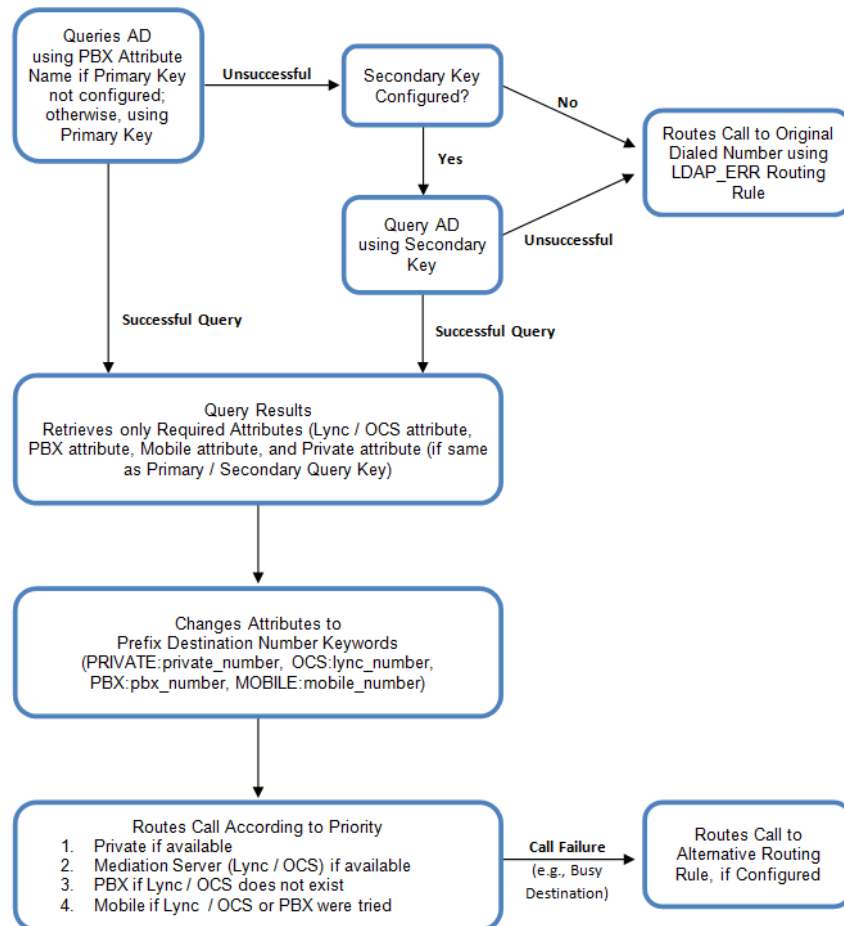
7. The device uses the Outbound IP Routing table to route the call based on the LDAP query result. The device routes the call according to the following priority:
  6. **Private line:** If the query is done for the private attribute and it's found, then the device routes the call according to this attribute.
  7. **Mediation Server SIP address (Lync / OCS):** If the private attribute does not exist or is not queried, then the device routes the call to the Mediation Server (which then routes the call to the Lync client).
  8. **PBX / IP PBX:** If the Lync / OCS client is not found in the AD, it routes the call to the PBX / IP PBX.
  9. **Mobile number:** If the Lync / OCS client (or Mediation Server) is unavailable (e.g., SIP response 404 "Not Found" upon INVITE sent to Lync client), and the PBX / IP PBX is also unavailable, then the device routes the call to the user's mobile number (if exists in the AD).
  10. **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.
  11. **"Redundant" route:** If the query failed (i.e., no attribute found in the AD), the device uses the routing rule matching the "LDAP\_ERR" prefix destination number value.



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

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

**Figure 19-4: LDAP Query Flowchart**



**Note:** If you are using the device's local LDAP cache, see 'Configuring the Device's LDAP Cache' on page 180 for the LDAP query process.

### 19.1.3.2 Configuring AD-Based Routing Rules

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

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

1. Configure the LDAP server parameters, as described in 'Configuring the LDAP Server' on page 179.
2. Configure the AD attribute names used in the LDAP query:
  - a. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Advanced Parameters**).

**Figure 19-5: LDAP Parameters for Microsoft Lync Server 2010**

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

- b. Configure the LDAP attribute names as desired.
  3. For the Gateway/IP-to-IP application: Configure AD-based Tel-to-IP routing rules:
    - a. Open the Outbound IP Routing Table page (Configuration tab > VoIP menu > GW and IP to IP submenu > Routing > Tel to IP Routing). For more information, see [Configuring Outbound IP Routing Table](#) on page 321.
    - b. Configure query-result routing rules for each IP domain (private, PBX / IP PBX, Lync / OCS clients, and mobile), using the LDAP keywords (case-sensitive) for the prefix destination number:
      - ◆ PRIVATE: Private number
      - ◆ OCS: Lync / OCS client number
      - ◆ PBX: PBX / IP PBX number
      - ◆ MOBILE: Mobile number
      - ◆ LDAP\_ERR: LDAP query failure
    - c. Configure a routing rule for routing the initial Tel call to the LDAP server, using the value "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.
  4. For the SBC application: Configure AD-based IP-to-IP routing rules:
    - a. Open the IP-to-IP Routing Table page (Configuration tab > VoIP menu > SBC submenu > Routing SBC > IP to IP Routing Table). For more information, see [Configuring SBC IP-to-IP Routing](#) on page 462.
    - b. Configure query-result routing rules for each IP domain (private, PBX / IP PBX, Lync / OCS clients, and mobile), using the LDAP keywords (case-sensitive) in the Destination Username Prefix field:
      - ◆ PRIVATE: Private number
      - ◆ OCS: Lync / OCS client number
      - ◆ PBX: PBX / IP PBX number
      - ◆ MOBILE: Mobile number
      - ◆ LDAP\_ERR: LDAP query failure
    - c. Configure a routing rule for routing the initial call (LDAP query) to the LDAP server, by setting the 'Destination Type' field to LDAP for denoting the IP address of the LDAP server.
    - d. For alternative routing, enable the alternative routing mechanism and configure corresponding SIP reasons for alternative routing. For this feature, alternative routing starts from the table row located under the LDAP query row.

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

#### AD-Based Tel-to-IP Routing Rule Configuration Examples

Index	Dest. Phone Prefix	Dest. IP Address
1	PRIVATE:	10.33.45.60
2	PBX:	10.33.45.65
3	OCS:	10.33.45.68
4	MOBILE:	10.33.45.100
5	LDAP_ERR	10.33.45.80
6	*	LDAP
7	*	10.33.45.72

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

#### AD-Based SBC IP-to-IP Routing Rule Configuration Examples

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

The configured routing rule example is explained below:

- **Rule 1:** Sends call to private telephone line (at 10.33.45.60) upon successful AD query result for the private attribute.
- **Rule 2:** Sends call to IP PBX (at 10.33.45.65) upon successful AD query result for the PBX attribute.
- **Rule 3:** Sends call to Lync client (i.e., Mediation Server at 10.33.45.68) upon successful AD query result for the Lync attribute.
- **Rule 4:** Sends call to user's mobile phone number (to PSTN through the device's IP address at 10.33.45.100) upon successful AD query result for the Mobile attribute.
- **Rule 5:** Sends call to IP address of device (10.33.45.80) if AD query failure (e.g., no response from LDAP server or attribute not found).
- **Rule 6:** Sends query for original destination number of received call to the LDAP server.

- **Rule 7:** Alternative routing rule that sends the call of original dialed number to IP destination 10.33.45.72. This rule is applied in any of the following cases
  - LDAP functionality is disabled.
  - LDAP query is successful but call fails (due to, for example, busy line) to all the relevant attribute destinations (private, Lync, PBX, and mobile), and a relevant Tel-to-IP Release Reason (see Alternative Routing for Tel-to-IP Calls on page 335) or SBC Alternative Routing Reason (see Configuring Alternative Routing Reasons on page 468) 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.

### 19.1.3.3 Querying the AD for Calling Name

The device can be configured to retrieve the calling name (display name) from Microsoft Active Directory (AD) for Tel-to-IP calls that are received without a calling name. The device queries the AD, based on the Calling Number search key and searches for the calling name attribute configured by the parameter, MSLDAPDisplayNameAttrName (e.g., "displayName"). The device uses the resultant calling name as the display name in the SIP From header of the sent INVITE message.

To configure this feature, the following keywords are used in the Calling Name Manipulation Table for Tel -> IP Calls table for the 'Prefix/Suffix to Add' fields, which can be combined with other characters:

- "\$LDAP-PBX": starts LDAP query using the MSLDAPPBXAttrName parameter as the search key
- "\$LDAP-MOBILE": starts LDAP query using MSLDAPMobileAttrName parameter as the search key

If the source (calling) number of the Tel-to-IP call matches the PBX / MOBILE (e.g., "telephoneNumber" and "mobile") number in the AD server, the device uses the resultant Display Name instead of the keyword(s).

For example, assume the following configuration in the Calling Name Manipulation Table for Tel -> IP Calls:

- 'Source Prefix' field is set to "4".
- 'Prefix to Add' field is set to "\$LDAP-PBX Office".

If the calling number is 4046 and the resultant LDAP query display name is "John Doe", the device sends the INVITE message with the following From header:

```
From: John Doe <sip:4064@company.com>\
```



#### Notes:

- The Calling Name Manipulation Table for Tel -> IP Calls table uses the numbers before manipulation, as inputs.
- The LDAP query uses the calling number after source number manipulation, as the search key value.



## 19.2 Least Cost Routing

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

### 19.2.1 Overview

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

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

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

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

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

**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
<b>A</b>	1	6	7	61
<b>B</b>	0	10	10	100
<b>C</b>	0.3	8	8.3	80.3
<b>D</b>	6	1	7	<b>16</b>

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

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

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

Two Cost Groups are configured as shown below:

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

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

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

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

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

- The following Cost Groups are configured:

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

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

Routing Index	Dest Phone Prefix	Destination IP	Cost Group ID
1	201	x.x.x.x	"A"
2	201	x.x.x.x	"B"
3	201	x.x.x.x	0
4	201	x.x.x.x	"B"

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

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

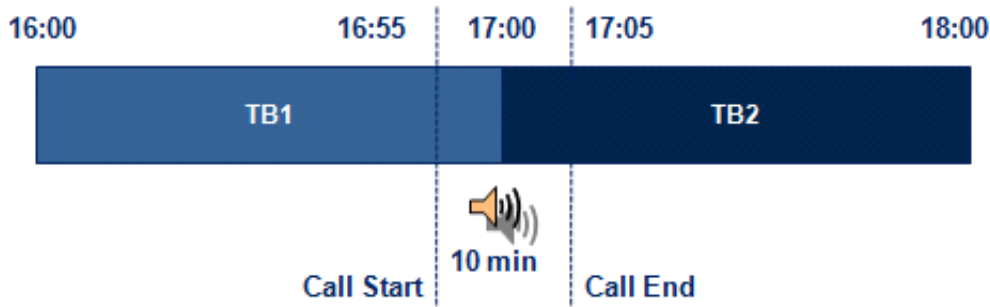
- **Example 3:** This example shows how the cost of a call is calculated if the call spans over multiple time bands:

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

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

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

**Figure 19-6: LCR using Multiple Time Bands (Example)**



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

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

## 19.2.2 Configuring LCR

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

1. Enable the LCR feature and configure the average call duration and default call connection cost - see 'Enabling LCR and Configuring Default LCR' on page 191.
2. Configure Cost Groups - see 'Configuring Cost Groups' on page 193.
3. Configure Time Bands for a Cost Group - see 'Configuring Time Bands for Cost Groups' on page 194.
4. Assign Cost Groups to outbound IP routing rules - see 'Assigning Cost Groups to Routing Rules' on page 196.

### 19.2.2.1 Enabling the LCR Feature

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

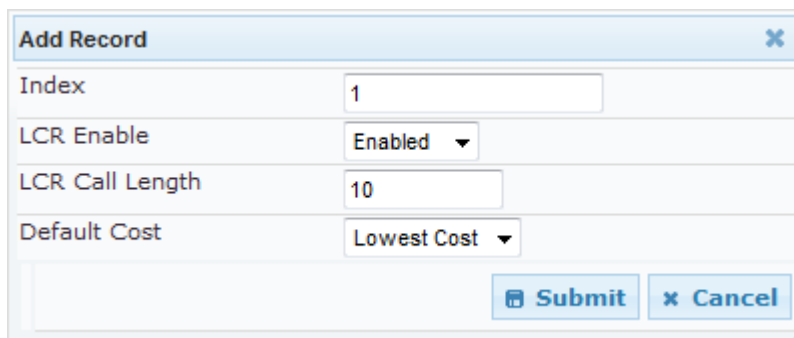


**Note:** The Routing Rule Groups table can also be configured using the table ini file parameter, RoutingRuleGroups or CLI command, configure voip > services least-cost-routing routing-rule-groups.

➤ **To enable LCR:**

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

**Figure 19-7: Routing Rule Groups Table - Add Record**



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

**Routing Rule Groups Table Description**

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

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

### 19.2.2.2 Configuring Cost Groups

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



**Note:** The Cost Group table can also be configured using the table ini file parameter, CostGroupTable or CLI command, configure voip > services least-cost-routing cost-group.

➤ **To configure Cost Groups:**

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

**Figure 19-8: Cost Group Table - Add Record**

Add Record	
Index	1
Cost Group Name	Local Calls
Default Connection Cost	2
Default Minute Cost	1
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

### Cost Group Table Description

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

### 19.2.2.3 Configuring Time Bands for Cost Groups

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



#### Notes:

- You cannot define overlapping time bands.
- The Time Band table can also be configured using the table ini file parameter, CostGroupTimebands or CLI command, configure voip >services least-cost-routing cost-group-time-bands.

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

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

Figure 19-9: Time Band Table - Add Record

Add Record	
Index	1
Start Time (ddd:hh:mm)	sat:06:00
End Time (ddd:hh:mm)	sun:22:00
Connection Cost	3
Minute Cost	0.5
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

#### Time Band Table Description

Parameter	Description
Index CLI: timeband-index <b>[CostGroupTimebands _TimebandIndex]</b>	Defines the table index entry.
Start Time CLI: start-time <b>[CostGroupTimebands _StartTime]</b>	Defines the day and time of day from when this time band is applicable. The format is ddd:hh:mm (e.g., sun:06:00), where: <ul style="list-style-type: none"> <li>ddd is the day (i.e., sun, mon, tue, wed, thu, fri, or sat)</li> <li>hh and mm denote the time of day, where hh is the hour (00-23) and mm the minutes (00-59)</li> </ul>
End Time CLI: end-time <b>[CostGroupTimebands _EndTime]</b>	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 CLI: connection-cost <b>[CostGroupTimebands _ConnectionCost]</b>	Defines the call connection cost during this time band. This is added as a fixed charge to the call. The valid value range is 0-65533. The default is 0. <b>Note:</b> The entered value must be a whole number (i.e., not a decimal).
Minute Cost CLI: minute-cost <b>[CostGroupTimebands _MinuteCost]</b>	Defines the call cost per minute charge during this timeband. The valid value range is 0-65533. The default is 0. <b>Note:</b> The entered value must be a whole number (i.e., not a decimal).

#### 19.2.2.4 Assigning Cost Groups to Routing Rules

Once you have configured your Cost Groups, you need to assign them to routing rules:

- Gateway/IP-to-IP application: Outbound IP Routing table - see Configuring Outbound IP Routing Table on page [321](#)
- SBC application: IP-to-IP Routing table - see Configuring SBC IP-to-IP Routing on page [462](#)



## 20 Enabling Applications

The device supports the following main applications:

- Stand-Alone Survivability (SAS) application (see SAS Overview on page 489)
- Session Border Control (SBC) application (see SBC Overview on page 419)
- Cloud Resilience Package (see CRP Overview on page 481)
- IP-to-IP application (see IP-to-IP Routing Overview on page 253)

The procedure below describes how to enable these applications. Once an application is enabled, the Web GUI provides menus and parameter fields relevant to the application.



### Notes:

- This page displays the application only if the device is installed with the relevant Software License Key supporting the application (see 'Software License Key' on page Software License Key on page 552).
- For enabling an application, a device reset is required.
- In some Web pages, the Gateway and IP-to-IP applications are denoted as "GW" and "IP2IP" respectively.

### ➤ To enable an application:

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** submenu > **Applications Enabling**).

▼		
⚡ SAS Application	Enable	▼
⚡ SBC Application	Enable	▼
⚡ IP to IP Application	Enable	▼

2. From the relevant application drop-down list, select **Enable**.
3. Save (burn) the changes to the device's flash memory with a device reset (see 'Saving Configuration' on page 532).

## Reader's Notes

## 21 Control Network

This section describes configuration of the network at the SIP control level.

### 21.1 Configuring SRD Table

The SRD Settings page allows you to configure up to 32 signaling routing domains (SRD). An SRD is configured with a unique name and assigned a Media Realm. Additional SBC attributes such as media anchoring and user registration can also be configured.

An SRD is a set of definitions together creating multiple, virtual multi-service IP gateways:

- Multiple and different SIP signaling interfaces (SRD associated with a SIP Interface) and RTP media (associated with a Media Realm) for multiple Layer-3 networks. Due to the B2BUA nature of the SBC application, different interfaces can be assigned to each leg of the call, and between the LAN and WAN side.
- Can operate with multiple gateway customers that may reside either in the same or in different Layer-3 networks as the device. This allows separation of signaling traffic between different customers. In such a scenario, the device is configured with multiple SRD's.

Typically, one SRD is defined for each group of SIP UAs (e.g. proxies, IP phones, application servers, gateways, and softswitches) that communicate with each other. This provides these entities with VoIP services that reside on the same Layer-3 network (must be able to communicate without traversing NAT devices and must not have overlapping IP addresses). One SRD is generally configured for the LAN and one for the WAN. Routing from one SRD to another is possible, whereby each routing destination (IP Group or destination address) indicates the SRD to which it belongs.

Once configured, you can use the SRD as follows:

- Associate it with a SIP Interface (see 'Configuring SIP Interface Table' on page 201)
- Associate it with an IP Group (see 'Configuring IP Groups' on page 204)
- Associate it with a Proxy Set (see 'Configuring Proxy Sets Table' on page 213)
- Apply an Admission Control rule to it (see 'Configuring Admission Control Table' on page 452)
- Define it as a Classification rule for the incoming SIP request (see 'Configuring Classification Rules' on page 456)
- Use it as a destination IP-to-IP routing rule (see 'Configuring SBC IP-to-IP Routing' on page 462)

The SRD Settings page also displays the IP Groups, Proxy Sets, and SIP Interfaces associated with a selected SRD index.



#### Notes:

- On the SRD Settings page, you can also configure a SIP Interface in the SIP Interface table, instead of navigating to the SIP Interface Table page as described in 'Configuring SIP Interface Table' on page 201.
- The SRD table can also be configured using the table ini file parameter, SRD or CLI command, `configure voip > control-network srd`.

➤ **To configure SRDs:**

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

**Figure 21-1: SRD Settings Page**

▼	
SRD Index	0 - Not Exist ▼
▼ Common Parameters	
SRD Name	<input type="text"/>
Media Realm	<input type="text"/>
▼ SBC Parameters	
Internal SRD Media Anchoring	Anchor Media ▼
Block Unregistered Users	No ▼
Max Number Of Registered Users	-1
Enable Un-Authenticated Registrations	Yes ▼

2. From the 'SRD Index' drop-down list, select an index for the SRD, and then configure it according to the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

**SRD Table Parameters**

Parameter	Description
SRD Name CLI: name [SRD_Name]	Mandatory descriptive name of the SRD. The valid value can be a string of up to 21 characters.
Media Realm CLI: media-realm [SRD_MediaRealm]	Defines the Media Realm associated with the SRD. The entered string value must be identical (and case-sensitive) to the Media Realm name configured in the Media Realm table (see 'Configuring Media Realms' on page 168). The valid value is a string of up to 40 characters. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ If the Media Realm is later deleted from the Media Realm table, then this value becomes invalid in the SRD table.</li> <li>▪ For configuring Media Realms, see 'Configuring Media Realms' on page 168.</li> </ul>
<b>SBC Parameters</b>	
Internal SRD Media Anchoring CLI: intra-srd-media-anchoring [SRD_IntraSRDMediaAnchoring]	Determines whether the device performs media anchoring or not on media for the SRD. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Anchor Media = (Default) RTP traverses the device and each leg uses a different coder or coder parameters.</li> <li>▪ <b>[1]</b> Don't Anchor Media = The RTP packet flow does not traverse the device; instead, the two SIP UA's establish a direct RTP/SRTP (media) flow between one another.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ When No Media Anchoring is enabled: <ul style="list-style-type: none"> <li>✓ The device does not perform manipulation on SDP data (offer/answer transactions) such as ports, IP address, and coders.</li> </ul> </li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>✓ Opening voice channels and allocation of IP media ports are not required.</li> <li>▪ When two UA's pertain to the same SRD and this parameter is set to <b>[1]</b>, and one of the UA's is defined as a foreign user (example, "follow me service") located on the WAN while the other UA is located on the LAN, then calls between these two UA's can't be established until this parameter is set to 0, as the device doesn't interfere in the SIP signaling. In other words, parameters such as IP addresses are not manipulated for calls between LAN and WAN (although required).</li> <li>▪ When the global parameter SBCDirectMedia is disabled, you cannot enable No Media Anchoring for two UA's pertaining to separate SRDs; No Media Anchoring can only be enable for two UA's pertaining to the same SRD.</li> <li>▪ For more information on media handling, see SBC Media Handling on page 425.</li> </ul>
Block Unregistered Users CLI: block-un-reg-users <b>[SRD_BlockUnRegUsers]</b>	<p>Determines whether the device blocks (rejects) incoming calls (INVITE requests) from unregistered users (pertaining to User-type IP Groups) for the SRD.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No = Calls from unregistered users are not blocked (default).</li> <li>▪ <b>[1]</b> Yes = Blocks calls from unregistered users.</li> </ul> <p><b>Note:</b> When the call is blocked, the device sends a SIP 500 "Server Internal Error" response to the remote end.</p>
Max Number of Registered Users CLI: max-reg-users <b>[SRD_MaxNumOfRegUsers]</b>	<p>Maximum number of users belonging to this SRD that can register with the device. By default, no limitation exists for registered users</p>
Enable Un-Authenticated Registrations CLI: enable-un-auth-registrs <b>[SRD_EnableUnAuthenticatedRegistrations]</b>	<p>Determines whether the device blocks REGISTER requests from new users (i.e., users not registered in the device's registration database) when the destination is a User-type IP Group.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No = The device sends REGISTER requests to the SIP proxy server and only if authenticated by the server does the device add the user registration to its database.</li> <li>▪ <b>[1]</b> Yes = The device adds REGISTER requests to its database even if the requests are not authenticated by a SIP proxy (default).</li> </ul>

## 21.2 Configuring SIP Interface Table

The SIP Interface table allows you to configure up to 32 SIP Interfaces. The SIP Interface defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface configured for the device (in the Multiple Interface table).

The SIP Interface is configured for a specific application (i.e., Gateway\IP-to-IP, SAS, and SBC) and associated with an SRD. For each SIP Interface, you can assign a SIP message policy, enable TLS mutual authentication, enable TCP keepalive, and determine the SIP response sent upon classification failure.

SIP Interfaces can be used, for example, for the following:

- Using SIP signaling interfaces per call leg (i.e., each SIP entity communicates with a specific SRD).
- Using different SIP listening ports for a single or for multiple IP network interfaces.
- Differentiating between applications by creating SIP Interfaces per application.

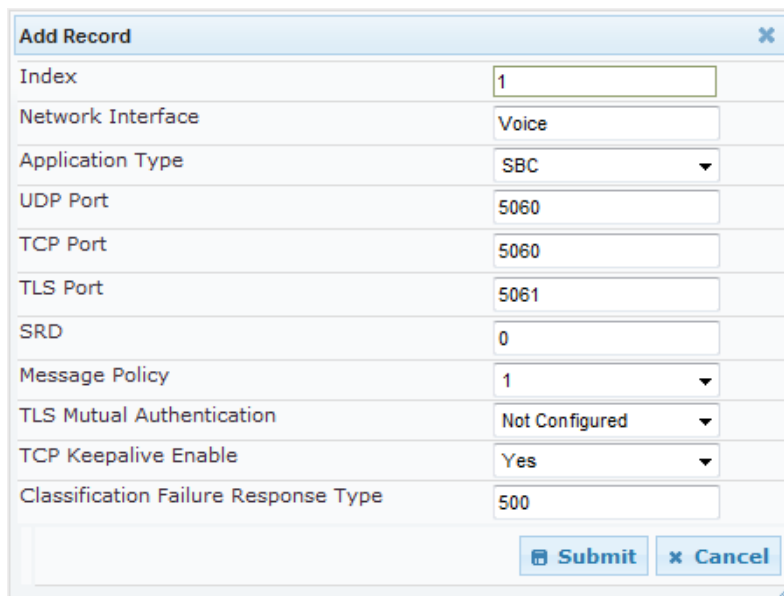
- Separating signaling traffic between networks (e.g., different customers) to use different routing tables, manipulations, SIP definitions, and so on.



**Note:** The SIP Interface table can also be configured using the table *ini* file parameter, SIPInterface or the CLI command, configure voip > control-network sip-interface.

➤ **To configure the SIP Interface table:**

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



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

### SIP Interface Table Parameters

Parameter	Description
<b>Network Interface</b> <b>[SIPInterface_NetworkInterface]</b> CLI: network-interface	Defines the Control-type IP network interface that you want to associate with the SIP Interface. This value string must be identical (including case-sensitive) to that configured in the 'Interface Name' field of the Multiple Interface table (see 'Configuring IP Network Interfaces' on page 107). The default is not configured. <b>Notes:</b> <ul style="list-style-type: none"> <li>■ SIP Interfaces that are assigned to a specific SRD must be defined with the same network interface. For example, if you define three SIP Interfaces for SRD ID #8, all these SIP Interfaces must be defined with the same network interface (e.g., "SIP1").</li> <li>■ To create a SIP interface on the WAN interface, enter the string "WAN". This WAN interface is selected in the Multiple Interface table (or use the WANInterfaceName parameter). If VLANs are defined for the WAN interface and one of the VLANs is selected as the VoIP WAN interface, then the defined SIP Interface uses this interface.</li> </ul>
<b>Application Type</b> <b>[SIPInterface_ApplicationType]</b>	Defines the application type associated with the SIP Interface.

Parameter	Description
<b>onType]</b> CLI: application-type	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> GW/IP2IP (default) = Gateway / IP-to-IP application.</li> <li>▪ <b>[1]</b> SAS = Stand-Alone Survivability (SAS) application.</li> <li>▪ <b>[2]</b> SBC = SBC application.</li> </ul>
UDP Port <b>[SIPInterface_UDPPort]</b> CLI: udp-port	Defines the listening and source UDP port. The valid range is 1 to 65534. The default is 5060. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ This port must be outside of the RTP port range.</li> <li>▪ Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).</li> </ul>
TCP Port <b>[SIPInterface_TCPPort]</b> CLI: tcp-port	Defines the listening TCP port. The valid range is 1 to 65534. The default is 5060. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ This port must be outside of the RTP port range.</li> <li>▪ Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).</li> </ul>
TLS Port <b>[SIPInterface_TLSPort]</b> CLI: tls-port	Defines the listening TLS port. The valid range is 1 to 65534. The default is 5061. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ This port must be outside of the RTP port range.</li> <li>▪ Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).</li> </ul>
SRD <b>[SIPInterface_SRD]</b> CLI: srd	Assigns an SRD ID to the SIP Interface. The default is 0. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ Each SRD can be associated with up to three SIP Interfaces, where each SIP Interface pertains to a different Application Type (GW/IP-to-IP, SAS, and SBC).</li> <li>▪ SIP Interfaces that are assigned to a specific SRD must be defined with the same network interface. For example, if you define three SIP Interfaces for SRD ID #8, all these SIP Interfaces must be defined with the same network interface (e.g., "SIP1").</li> <li>▪ To configure SRDs, see 'Configuring SRD Table' on page <a href="#">199</a>.</li> </ul>
Message Policy <b>[SIPInterface_Message Policy]</b> CLI: message-policy	Assigns a SIP message policy to the SIP interface. <b>Note:</b> To configure SIP message policies, see 'Configuring SIP Message Policy Rules'.
TLS Mutual Authentication <b>[SIPInterface_TLSMutualAuthentication]</b> CLI: tls-mutual-auth	Enables TLS mutual authentication per SIP Interface. <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured = (Default) The SIPRequireClientCertificate global parameter setting is applied.</li> <li>▪ <b>[0]</b> Disable = Device does not request the client certificate for TLS connection.</li> <li>▪ <b>[1]</b> Enable = Device requires receipt and verification of the client certificate to establish the TLS connection.</li> </ul>

Parameter	Description
TCP Keepalive Enable <b>[SIPInterface_TCPKeepaliveEnable]</b> CLI: tcp-keepalive-enable	<p>Enables the TCP Keep-Alive mechanism with the IP entity on this SIP interface. TCP keepalive can be used, for example, to keep a NAT entry open for clients located behind a NAT server or simply to check that the connection to the IP entity is available.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No (default)</li> <li>▪ <b>[1]</b> Yes</li> </ul> <p><b>Note:</b> For configuring TCP keepalive, use the following ini file parameters: TCP TCPKeepAliveTime, TCPKeepAliveInterval, and TCPKeepAliveRetry.</p>
Classification Failure Response Type <b>[SIPInterface_ClassificationFailureResponseType]</b> CLI: classification_fail_response_type	<p>Defines the SIP response code that the device sends if a received SIP request (OPTIONS, REGISTER, or INVITE) has failed the classification process.</p> <p>The valid value can be a SIP response code from 400 through 699, or it can be set to 0 to not send any response at all. The default response code is 500 (Server Internal Error).</p> <p>This feature is important for preventing Denial of Service (DoS) attacks, typically initiated from the WAN. Malicious attackers can use SIP scanners to detect ports used by SIP devices. These scanners scan devices by sending UDP packets containing a SIP request to a range of specified IP addresses, listing those that return a valid SIP response. Once the scanner finds a device that supports SIP, it extracts information from the response and identifies the type of device (IP address and name) and can execute DoS attacks. A way to defend the device against such attacks is to not send a SIP reject response to these unclassified "calls" so that the attacker assumes that no device exists at such an IP address and port.</p> <p><b>Note:</b> This parameter is applicable only if the device is set to reject unclassified calls. This is configured using the 'Unclassified Calls' parameter on the General Settings page (<b>Configuration</b> tab &gt; <b>VoIP</b> menu &gt; <b>SBC</b> &gt; <b>General Settings</b>).</p>

## 21.3 Configuring IP Groups

The IP Group Table page allows you to create up to 32 IP Groups. The IP Group represents a SIP entity on the network with which the device communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set (see 'Configuring Proxy Sets Table' on page 213).

For the SBC application, this table can also be used to classify incoming SIP dialog-initiating requests (e.g., INVITE messages) to specific IP Groups based on the associated Proxy Set ID. However, it is highly recommended to use the Classification table for classifying incoming SIP dialogs to the IP Groups (see 'Configuring Classification Rules' on page 456). See the 'Classify by Proxy Set' parameter below for a detailed description of this feature and for important recommendations.

For the SBC application, IP Groups are used for IP-to-IP routing rules where they represent the source and destination of the call (see 'Configuring SBC IP-to-IP Routing' on page 462).

For the Gateway/IP-to-IP application, IP Groups are used for the following:

- SIP dialog registration and authentication (digest user/password) of a specific IP Group (Served IP Group, e.g., corporate IP-PBX) with another IP Group (Serving IP Group, e.g., ITSP). This is configured in the Account table (see Configuring Account Table on page 219).



- Call routing rules:
  - Outgoing IP calls (IP-to-IP or Tel-to-IP): The IP Group identifies the source of the call and is used as the destination of the outgoing IP call (defined in the Outbound IP Routing Table). For Tel-to-IP calls, the IP Group (Serving IP Group) can be used as the IP destination to where all SIP dialogs that are initiated from a Trunk Group are sent (defined in Configuring Hunt Group Settings on page 291).
  - Incoming IP calls (IP-to-IP or IP-to-Tel): The IP Group identifies the source of the IP call.
  - Number Manipulation rules to IP: The IP Group is used to associate the rule with specific calls identified by IP Group.

**Notes:**

- IP Group ID 0 cannot be used. This IP Group is set to default values and is used by the device when IP Groups are not implemented.
- When operating with multiple IP Groups, the default Proxy server must not be used (i.e., the parameter IsProxyUsed must be set to 0).
- If different SRDs are configured in the IP Group and Proxy Set tables, the SRD defined for the Proxy Set takes precedence.
- You can also configure the IP Groups table using the table ini file parameter, IPGroup (see 'Configuration Parameters Reference' on page 661) or CLI command, configure voip > control- network ip-group.

➤ **To configure IP Groups:**

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

**Figure 21-2: IP Group Table - Add Dialog Box**

Common	
Index	0
Type	Server
Description	
Proxy Set ID	-1
SIP Group Name	
Contact User	
Local Host Name	
SRD	0
Media Realm Name	
IP Profile ID	0
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Configure the IP Group parameters according to the table below.
4. Click **Submit**.
5. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## IP Group Parameters

Parameter	Description
<b>Common Parameters</b>	
Type CLI: type <b>[IPGroup_Type]</b>	<p>Defines the type of IP Group:</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Server = Used when the destination address, configured by the Proxy Set, of the IP Group (e.g., ITSP, Proxy, IP-PBX, or Application server) is known.</li> <li>▪ <b>[1]</b> 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) users.</li> </ul> <p>Typically, this IP Group is configured with a Serving IP Group that represents an IP-PBX, Application or Proxy server that serves this User-type IP Group. Each SIP request sent by a user of this IP Group is proxied to the Serving IP Group. For registrations, the device updates its internal database with the AOR and contacts of the users. Digest authentication using SIP 401/407 responses (if needed) is performed by the Serving IP Group. The device forwards these responses directly to the SIP users.</p> <p>To route a call to a registered user, a rule must be configured in the Outbound IP Routing Table or SBC IP-to-IP Routing table. The device searches the dynamic database (by using the request URI) for an entry that matches a registered AOR or Contact. Once an entry is found, the IP destination is obtained from this entry, and a SIP request is sent to the destination.</p> <p>The device also supports NAT traversal for the SIP clients located behind NAT. In this case, the device must be defined with a global IP address.</p> <ul style="list-style-type: none"> <li>▪ <b>[2]</b> Gateway = This is applicable only to the SBC application in scenarios where the device receives requests to and from a gateway representing multiple users. This IP Group type is necessary as the other IP Group types are not suitable: <ul style="list-style-type: none"> <li>✓ The IP Group cannot be defined as a Server since its destination address is unknown during configuration.</li> <li>✓ The IP Group cannot be defined as a User since the SIP Contact header of the incoming REGISTER does not represent a specific user. The Request-URI user part can change and therefore, the device is unable to identify an already registered user and therefore, adds an additional record to the database.</li> </ul> </li> </ul> <p>The IP address of the Gateway IP Group is obtained dynamically from the host part of the Contact header in the REGISTER request received from the IP Group. Therefore, routing to this IP Group is possible only once a REGISTER request is received. If a REGISTER refresh request arrives, the device updates the new location (i.e., IP address) of the IP Group. If the REGISTER fails, no update is performed. If an UN-REGISTER request arrives, the IP address associated with the IP Group is deleted and therefore, no routing to the IP Group is done.</p> <p><b>Note:</b> This field is applicable only to the SBC or IP-to-IP application.</p>
Description CLI: description <b>[IPGroup_Description]</b>	<p>Defines a brief description for the IP Group.</p> <p>The valid value is a string of up to 29 characters. The default is an empty field.</p>

Parameter	Description
Proxy Set ID CLI: proxy-set-id <b>[IPGroup_ProxySetId]</b>	<p>Assigns a Proxy Set ID to the IP Group. All INVITE messages destined to this IP Group are sent to the IP address configured for the Proxy Set.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Proxy Set ID 0 must <b>not</b> be used; this is the device's default Proxy.</li> <li>The Proxy Set is applicable only to Server-type IP Groups.</li> <li>The SRD configured for this Proxy Set in the Proxy Set table is automatically assigned to this IP Group (see the 'SRD' field below).</li> <li>To configure Proxy Sets, see 'Configuring Proxy Sets Table' on page <a href="#">213</a>.</li> </ul>
SIP Group Name CLI: sip-group-name <b>[IPGroup_SIPGroupName]</b>	<p>Defines the SIP Request-URI host name used in INVITE and REGISTER messages sent to this IP Group, or the host name in the From header of INVITE messages received from this IP Group.</p> <p>The valid value is a string of up to 100 characters. The default is an empty field.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If this parameter is not configured, the value of the global parameter, ProxyName is used instead (see 'Configuring Proxy and Registration Parameters' on page <a href="#">222</a>).</li> <li>If the IP Group is of User type, this parameter is used internally as a host name in the Request-URI for Tel-to-IP initiated calls. For example, if an incoming call from the device's T1 trunk is routed to a User-type IP Group, the device first creates the Request-URI (&lt;destination_number&gt;@&lt;SIP Group Name&gt;), and then it searches the internal database for a match.</li> </ul>
Contact User CLI: contact-user <b>[IPGroup_ContactUser]</b>	<p>Defines the user part of the From, To, and Contact headers of SIP REGISTER messages, and the user part of the Contact header of INVITE messages received from this IP Group and forwarded by the device to another IP Group.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to Server-type IP Groups.</li> <li>This parameter is overridden by the 'Contact User' parameter in the 'Account' table (see 'Configuring Account Table' on page <a href="#">219</a>).</li> </ul>
Local Host Name CLI: local-host-name <b>[IPGroup_ContactName]</b>	<p>Defines the host name (string) that the device uses in the SIP message's Via and Contact headers. This is typically used to define an FQDN as the host name. The device uses this string for Via and Contact headers in outgoing INVITE messages to a specific IP Group, and the Contact header in SIP 18x and 200 OK responses for incoming INVITE messages from a specific IP Group. The Inbound IP Routing table can be used to identify the source IP Group from where the INVITE message was received.</p> <p>If this parameter is not configured (default), these headers are populated with the device's dotted-decimal IP address of the network interface on which the message is sent.</p> <p><b>Note:</b> To ensure proper device handling, this parameter should be a valid FQDN.</p>

Parameter	Description
SRD CLI: srd [IPGroup_SRD]	Assigns an SRD to the IP Group. The default is 0. <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>To configure SRDs, see Configuring SRD Table on page 199.</li> <li>For Server-type IP Groups, if you assign the IP Group with a Proxy Set ID (in the 'Proxy Set ID' field), the SRD field is automatically set to the SRD value assigned to the Proxy Set in the Proxy Set table.</li> </ul>
Media Realm Name CLI: media-realm-name [IPGroup_MediaRealm]	Assigns a Media Realm to the IP Group. The string value must be identical (including case-sensitive) to the Media Realm name defined in the Media Realm table. <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>If the Media Realm is later deleted from the Media Realm table, then this value becomes invalid.</li> <li>For configuring Media Realms, see Configuring Media Realms on page 168.</li> </ul>
IP Profile ID CLI: ip-profile-id [IPGroup_ProfileId]	Assigns an IP Profile to the IP Group. The default is 0. <b>Note:</b> To configure IP Profiles, see 'Configuring IP Profiles' on page 239.
<b>Gateway Parameters</b>	
Always Use Route Table CLI: always-use-route-table [IPGroup_AlwaysUseRouteTable]	Defines the Request-URI host name in outgoing INVITE messages. <ul style="list-style-type: none"> <li><b>[0]</b> No (default).</li> <li><b>[1]</b> Yes = The device uses the IP address (or domain name) defined in the Outbound IP Routing Table (see Configuring the Outbound IP Routing Table on page 321) as the Request-URI host name in outgoing INVITE messages, instead of the value configured in the 'SIP Group Name' field.</li> </ul> <b>Note:</b> This parameter is applicable only to Server-type IP Groups.
Routing Mode CLI: routing-mode [IPGroup_RoutingMode]	Defines the routing mode for outgoing SIP INVITE messages. <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured = (Default) The routing is according to the selected Serving IP Group. If no Serving IP Group is selected, the device routes the call according to the Outbound IP Routing Table (see Configuring Outbound IP Routing Table on page 321).</li> <li><b>[0]</b> Routing Table = The device routes the call according to the Outbound IP Routing Table.</li> <li><b>[1]</b> Serving IP Group = The device sends the SIP INVITE to the selected Serving IP Group. If no Serving IP Group is selected, the default IP Group is used. If the Proxy server(s) associated with the destination IP Group is not alive, the device uses the Outbound IP Routing Table (if the parameter IsFallbackUsed is set 1, i.e., fallback enabled - see 'Configuring Proxy and Registration Parameters' on page 222).</li> <li><b>[2]</b> Request-URI = The device sends the SIP INVITE to the IP address according to the received SIP Request-URI host name.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to the IP-to-IP application.</li> <li>This parameter is applicable only to Server-type IP Groups.</li> </ul>
SIP Re-Routing Mode	Defines the routing mode after a call redirection (i.e., a 3xx SIP response

Parameter	Description
CLI: re-routing-mode <b>[IPGroup_SIPReRouting Mode]</b>	<p>is received) or transfer (i.e., a SIP REFER request is received).</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured (Default)</li> <li>▪ <b>[0]</b> Standard = INVITE messages that are generated as a result of Transfer or Redirect are sent directly to the URI, according to the Refer-To header in the REFER message or Contact header in the 3xx response.</li> <li>▪ <b>[1]</b> Proxy = Sends a new INVITE to the Proxy. This is applicable only if a Proxy server is used and the parameter AlwaysSendtoProxy is set to 0.</li> <li>▪ <b>[2]</b> Routing Table = Uses the Routing table to locate the destination and then sends a new INVITE to this destination.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ When this parameter is set to <b>[1]</b> and the INVITE sent to the Proxy fails, the device re-routes the call according to the Standard mode <b>[0]</b>.</li> <li>▪ When this parameter is set to <b>[2]</b> and the INVITE fails, the device re-routes the call according to the Standard mode <b>[0]</b>. If DNS resolution fails, the device attempts to route the call to the Proxy. If routing to the Proxy also fails, the Redirect / Transfer request is rejected.</li> <li>▪ When this parameter is set to <b>[2]</b>, the XferPrefix parameter can be used to define different routing rules for redirected calls.</li> <li>▪ This parameter is ignored if the parameter AlwaysSendToProxy is set to 1.</li> </ul>
Enable Survivability CLI: enable-survivability <b>[IPGroup_EnableSurvivability]</b>	<p>Defines how the device handles registration messages and whether Survivability mode is enabled for User-type IP Groups.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default).</li> <li>▪ <b>[1]</b> Enable if Necessary = Survivability mode is enabled only if the Serving IP Group is unavailable. The device saves in its Registration database the registration messages sent by the clients (e.g., IP phones) belonging to the User-type IP Group. If communication with the Serving IP Group (e.g., IP-PBX) fails, the User-type IP Group enters into Survivability mode in which the device uses its database for routing calls between the clients of the User-type IP Group. In Survivability mode, the RTP packets between the clients always traverse through the device, and new registrations can also be processed. When the Serving IP Group is available again, the device returns to normal mode, sending INVITE and REGISTER messages to the Serving IP Group.</li> <li>▪ <b>[2]</b> Always Enable = Survivability mode is always enabled. The communication with the Serving IP Group is always considered as failed. The device uses its database for routing calls between the clients of the User-type IP Group.</li> <li>▪ <b>[3]</b> Always Terminate Register = The registration messages received from the clients are saved in the device's registration database without forwarding them to the proxy server. Upon receipt of the registration message, the device returns a SIP 200 OK to the client.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to the IP-to-IP application.</li> <li>▪ This parameter is applicable only to User-type IP Groups.</li> </ul>
Serving IP Group ID CLI: serving-ip-group-id <b>[IPGroup_ServingIPGroup]</b>	<p>If configured, INVITE messages initiated from the IP Group are sent to this Serving IP Group (range 1 to 9). In other words, the INVITEs are sent to the address defined for the Proxy Set associated with this Serving IP Group. The Request-URI host name in the INVITE messages</p>

Parameter	Description
	<p>are set to the value of the 'SIP Group Name' parameter defined for the Serving IP Group.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the IP-to-IP application.</li> <li>If the PreferRouteTable parameter is set to 1, the routing rules in the Outbound IP Routing Table take precedence over this 'Serving IP Group ID' parameter.</li> <li>If this parameter is not configured, the INVITE messages are sent to the default Proxy or according to the 'Outbound IP Routing Table'.</li> </ul>
<b>SBC Parameters</b>	
Classify By Proxy Set CLI: classify-by-proxy-set <b>[IPGroup_ClassifyByProxySet]</b>	<p>Defines whether the incoming INVITE is classified to an IP Group according to its associated Proxy Set ID.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul> <p>This classification occurs only if classification according to the device's database fails to (i.e., received INVITE is not from a registered user). The classification proceeds with checking whether the INVITE's IP address (if host names, then according to the dynamically resolved IP address list) is defined for a Proxy Set ID (in the Proxy Set table). If a Proxy Set ID has such an IP address, the device classifies the INVITE as belonging to the IP Group associated with this Proxy Set. The Proxy Set ID is assigned to the IP Group using the IP Group table's 'Proxy Set ID' parameter (see above).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>In cases where multiple IP Groups are associated with the same Proxy Set ID, do not enable this feature. If enabled, the device is unable to correctly classify the incoming INVITES to the appropriate IP Groups.</li> <li>To enhance security, it is highly recommended to disable this parameter so that the device can use the Classification table rules to classify the call. If this parameter is enabled, the Classification table is not used if an associated Proxy Set is found.</li> <li>This parameter is applicable only to Server-type IP Groups.</li> </ul>
Max Number Of Registered Users CLI: max-num-of-reg-users <b>[IPGroup_MaxNumOfRegUsers]</b>	<p>Defines the maximum number of users in this IP Group that can register with the device. By default, no limitation exists for registered users.</p> <p><b>Note:</b> This field is applicable only to User-type IP Groups.</p>
Source URI Input CLI: src-uri-input <b>[IPGroup_SourceUriInput]</b>	<p>Defines the SIP header in the incoming INVITE to use for call matching characteristics based on source URIs.</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured (default)</li> <li><b>[0]</b> From</li> <li><b>[1]</b> To</li> <li><b>[2]</b> Request-URI</li> <li><b>[3]</b> P-Asserted - First Header</li> <li><b>[4]</b> P-Asserted - Second Header</li> <li><b>[5]</b> P-Preferred</li> <li><b>[6]</b> Route</li> <li><b>[7]</b> Diversion</li> <li><b>[8]</b> P-Associated-URI</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[9]</b> P-Called-Party-ID</li> <li>▪ <b>[10]</b> Contact</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only when classification is done according to the Classification table.</li> <li>▪ If the configured SIP header does not exist in the incoming INVITE message, the classification of the message to a source IP Group fails.</li> <li>▪ If the device receives an INVITE as a result of a REFER request or a 3xx response, then the incoming INVITE is routed according to the Request-URI. The device identifies such INVITEs according to a specific prefix in the Request-URI header, configured by the SBCXferPrefix parameter. Therefore, in this scenario, the device ignores this parameter setting.</li> </ul>
Destination URI Input CLI: dst-uri-input <b>[IPGroup_DestUriInput]</b>	<p>Defines the SIP header in the incoming INVITE used for call matching characteristics based on destination URIs.</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured (default)</li> <li>▪ <b>[0]</b> From</li> <li>▪ <b>[1]</b> To</li> <li>▪ <b>[2]</b> Request-URI</li> <li>▪ <b>[3]</b> P-Asserted - First Header</li> <li>▪ <b>[4]</b> P-Asserted - Second Header</li> <li>▪ <b>[5]</b> P-Preferred</li> <li>▪ <b>[6]</b> Route</li> <li>▪ <b>[7]</b> Diversion</li> <li>▪ <b>[8]</b> P-Associated-URI</li> <li>▪ <b>[9]</b> P-Called-Party-ID</li> <li>▪ <b>[10]</b> Contact</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only when classification is done according to the Classification table.</li> <li>▪ If the configured SIP header does not exist in the incoming INVITE message, the classification of the message to a source IP Group fails.</li> <li>▪ If the device receives an INVITE as a result of a REFER request or a 3xx response, then the incoming INVITE is routed according to the Request-URI. The device identifies such INVITEs according to a specific prefix in the Request-URI header, configured by the SBCXferPrefix parameter. Therefore, in this scenario, the device ignores this parameter setting.</li> </ul>
Inbound Message Manipulation Set CLI: inbound-mesg-manipulation-set <b>[IPGroup_InboundManSet]</b>	<p>Assigns a Message Manipulation Set (rule) to the IP Group for SIP message manipulation on the inbound message. The Message Manipulation rules are configured using the MessageManipulations parameter (see Configuring SIP Message Manipulation on page <a href="#">226</a>).</p>
Outbound Message Manipulation Set CLI: outbound-mesg-manipulation-set <b>[IPGroup_OutboundManSet]</b>	<p>Message Manipulation Set (rule) that you want to assign to this IP Group for SIP message manipulation on the outbound message. The Message Manipulation rules are configured using the MessageManipulations parameter (see Configuring SIP Message Manipulation on page <a href="#">226</a>).</p>



Parameter	Description
Registration Mode CLI: registration-mode <b>[IPGroup_RegistrationMode]</b>	Defines the registration mode for the IP Group: <ul style="list-style-type: none"> <li>▪ <b>[0]</b> User initiates registrations (default)</li> <li>▪ <b>[1]</b> SBC initiate registrations = Used when the device serves as a client (e.g., with an IP PBX). This functions only with User Info file.</li> <li>▪ <b>[2]</b> No registrations needed = The device adds users to its database in active state.</li> </ul>
Authentication Mode CLI: authentication-mode <b>[IPGroup_AuthenticationMode]</b>	Defines the authentication mode. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> User Authenticates = (Default) The device does not handle the authentication, but simply passes the authentication messages between the SIP user agents.</li> <li>▪ <b>[1]</b> SBC as client = The device authenticates as a client. It receives the 401/407 response from the proxy requesting for authentication. The device sends the proxy the authorization credentials (i.e., user name and password) according to one of the following: 1) account defined in the Account table (only if authenticating Server-type IP Group), 2) global username and password parameters (only if authenticating Server-type IP Group), 3) User Information file, or 4) sends request to users requesting credentials (only if authenticating User-type IP Group).</li> <li>▪ <b>[2]</b> SBC as Server = The device authenticates as a server (using the User Information file).</li> </ul>
Authentication Method List CLI: authentication-method-list <b>[IPGroup_MethodList]</b>	Defines SIP methods that the device must challenge. Multiple entries are separated by the backslash "\". If you set this parameter to an empty value, no methods are challenged. The default value is "INVITE\REGISTER". <b>Note:</b> This parameter is applicable only if the 'Authentication Mode' parameter is set to SBC as Server [2].
Enable SBC Client Forking Mode CLI: enable-sbc-client-forking <b>[IPGroup_EnableSBCClientForking]</b>	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. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Sequential = (Default) Sequentially sends the INVITE to each contact. If there is no answer from the first contact, it sends the INVITE to the second contact, and so on until a contact answers. If no contact answers, the call fails or is routed to an alternative destination, if configured.</li> <li>▪ <b>[1]</b> Parallel = Sends the INVITE simultaneously to all contacts. The call is established with the first contact that answers.</li> <li>▪ <b>[2]</b> Sequential Available Only = Sequentially sends the INVITE only to available contacts (i.e., not busy). If there is no answer from the first available contact, it sends the INVITE to the second contact, and so on until a contact answers. If no contact answers, the call fails or is routed to an alternative destination, if configured.</li> </ul> <b>Note:</b> The device can also fork INVITE messages received for a Request-URI of a specific contact (user) registered in the database to all other users located under the same AoR as the specific contact. This is configured using the SBCSendInviteToAllContacts parameter..



## 21.4 Configuring Proxy Sets Table

The Proxy Sets Table page allows you to define *Proxy Sets*. A Proxy Set is a group of Proxy servers defined by IP address or fully qualified domain name (FQDN). You can define up to 32 Proxy Sets, each with up to five Proxy server addresses. For each Proxy server address you can define the transport type (i.e., UDP, TCP, or TLS). In addition, Proxy load balancing and redundancy mechanisms can be applied per Proxy Set if it contains more than one Proxy address.

Proxy Sets can later be assigned to Server-type IP Groups (see 'Configuring IP Groups' on page 204). When the device sends an INVITE message to an IP Group, it is sent to the IP address or domain name defined for the Proxy Set that is associated with the IP Group. In other words, the Proxy Set represents the **destination** of the call. Typically, for IP-to-IP call routing, at least two Proxy Sets are defined for call destination – one for each leg (IP Group) of the call (i.e., both directions). For example, one Proxy Set for the Internet Telephony Service provider (ITSP) interfacing with one 'leg' of the device and another Proxy Set for the second SIP entity (e.g., ITSP) interfacing with the other 'leg' of the device.



### Notes:

- Proxy Sets can be assigned only to Server-type IP Groups.
- To enable classification of IP Groups according to Proxy Set ID, in the IP Group table, set the 'Classify By Proxy Set' parameter to Enable.
- The Proxy Set table can also be configured using two complementary tables:
  - Proxy Set ID with IP addresses: Table ini file parameter, ProxyIP or CLI command, configure voip > control-network proxy-ip > proxy-set-id.
  - Attributes for the Proxy Set: Table ini file parameter, ProxySet or CLI command, configure voip > control-network proxy-set.

### ➤ To configure Proxy Sets:

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).

Figure 21-3: Proxy Sets Table Page

Proxy Set ID	
Proxy Set ID	1

	Proxy Address	Transport Type
1	100.33.2.26	UDP
2		
3		
4		
5		

Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	10
Proxy Load Balancing Method	Round Robin
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	1
Classification Input	IP only

2. From the 'Proxy Set ID' drop-down list, select an ID for the desired group.
3. Configure the Proxy parameters, as required. For a description of the parameters, see the table below.
4. Click **Submit**.
5. To save the changes to flash memory, see 'Saving Configuration' on page 532.

**Proxy Sets Table Parameters**

Parameter	Description
Web: Proxy Set ID EMS: Index CLI: configure voip > control-network proxy-set <b>[ProxySet_Index]</b>	<p>Defines the Proxy Set identification number.</p> <p>The valid value is 0 to 31. Proxy Set ID 0 is used as the default Proxy Set.</p> <p><b>Note:</b> Although not recommended, you can use both default Proxy Set (ID 0) and IP Groups for call routing. For example, in the Trunk Group Settings page (see Configuring Hunt Group Settings on page 291) you can configure a Serving IP Group to where you want to route specific Trunk Group channels, and all other device channels then use the default Proxy Set. You can also use IP Groups in the Outbound IP Routing Table (see Configuring the Outbound IP Routing Table on page 321) to configure the default Proxy Set if the parameter PreferRouteTable is set to 1.</p> <p>To summarize, if the default Proxy Set is used, the INVITE message is sent according to the following preferences:</p> <ul style="list-style-type: none"> <li>▪ To the Trunk Group's Serving IP Group ID, as defined in the Trunk Group Settings table.</li> <li>▪ According to the Outbound IP Routing Table if the parameter PreferRouteTable is set to 1.</li> <li>▪ To the default Proxy.</li> </ul> <p>Typically, when IP Groups are used, there is no need to use the default Proxy and all routing and registration rules can be configured using IP Groups and the Account tables (see 'Configuring Account Table' on page 219).</p>
Proxy Address CLI: control-network proxy-ip > proxy-address <b>[ProxyIp_IpAddress]</b>	<p>Defines the address (and optionally, port number) of the Proxy server. Up to five addresses can be configured per Proxy Set.</p> <p>The address can be defined as an IP address in dotted-decimal notation (e.g., 201.10.8.1) or as an FQDN. You can also specify the selected port in the format, &lt;IP address&gt;:&lt;port&gt;.</p> <p>If you enable Proxy Redundancy (by setting the parameter EnableProxyKeepAlive to 1 or 2), the device can operate with multiple Proxy servers. If there is no response from the first (<i>primary</i>) Proxy defined in the list, the device attempts to communicate with the other (<i>redundant</i>) Proxies in the list. When a redundant Proxy is located, the device either continues operating with it until the next failure occurs or reverts to the primary Proxy (refer to the parameter ProxyRedundancyMode). If none of the Proxy servers respond, the device goes over the list again.</p> <p>The device also provides real-time switching (Hot-Swap mode) between the primary and redundant proxies (refer to the parameter IsProxyHotSwap). If the first Proxy doesn't respond to the INVITE message, the same INVITE message is immediately sent to the next Proxy in the list. The same logic applies to REGISTER messages (if RegistrarIP is not defined).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If EnableProxyKeepAlive is set to 1 or 2, the device monitors the connection with the Proxies by using keep-alive messages (OPTIONS or REGISTER).</li> <li>▪ To use Proxy Redundancy, you must specify one or more redundant</li> </ul>

Parameter	Description
	<p>Proxies.</p> <ul style="list-style-type: none"> <li>When a port number is specified (e.g., domain.com:5080), DNS NAPTR/SRV queries aren't performed, even if ProxyDNSQueryType is set to 1 or 2.</li> </ul>
<p>Transport Type CLI: control-network proxy-ip &gt; transport-type <b>[ProxyIp_TransportType]</b></p>	<p>Defines the transport type of the proxy server.</p> <ul style="list-style-type: none"> <li><b>[0]</b> UDP</li> <li><b>[1]</b> TCP</li> <li><b>[2]</b> TLS</li> <li><b>[-1]</b> = Undefined</li> </ul> <p><b>Note:</b> If no transport type is selected, the value of the global parameter SIPTransportType is used.</p>
<p>Web/EMS: Enable Proxy Keep Alive CLI: control-network proxy-set &gt; proxy-enable-keep-alive <b>[ProxySet_EnableProxyKeepAlive]</b></p>	<p>Enables the Keep-Alive mechanism with the Proxy server(s).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> Using Options = Enables Keep-Alive with Proxy using SIP OPTIONS messages.</li> <li><b>[2]</b> Using Register = Enables Keep-Alive with Proxy using SIP REGISTER messages.</li> </ul> <p>If set to 'Using Options', the SIP OPTIONS message is sent every user-defined interval (configured by the parameter ProxyKeepAliveTime). If set to 'Using Register', the SIP REGISTER message is sent every user-defined interval (configured by the RegistrationTime parameter for the Gateway/IP-to-IP application or SBCProxyRegistrationTime parameter for SBC application). Any response from the Proxy, either success (200 OK) or failure (4xx response) is considered as if the Proxy is communicating correctly.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For Survivability mode for User-type IP Groups, this parameter must be enabled (1 or 2).</li> <li>This parameter must be set to 'Using Options' when Proxy redundancy is used.</li> <li>When this parameter is set to 'Using Register', the homing redundancy mode is disabled.</li> <li>When the active proxy doesn't respond to INVITE messages sent by the device, the proxy is tagged as 'offline'. The behavior is similar to a Keep-Alive (OPTIONS or REGISTER) failure.</li> <li>If this parameter is enabled and the proxy uses the TCP/TLS transport type, you can enable CRLF Keep-Alive mechanism, using the UsePingPongKeepAlive parameter.</li> </ul>
<p>Web: Proxy Keep Alive Time EMS: Keep Alive Time CLI: control-network proxy-set &gt; proxy-keep-alive-time <b>[ProxySet_ProxyKeepAliveTime]</b></p>	<p>Defines the Proxy keep-alive time interval (in seconds) between Keep-Alive messages.</p> <p>The valid range is 5 to 2,000,000. The default is 60.</p> <p><b>Note:</b> This parameter is applicable only if the parameter EnableProxyKeepAlive is set to 1 (OPTIONS). When the parameter EnableProxyKeepAlive is set to 2 (REGISTER), the time interval between Keep-Alive messages is determined by the RegistrationTime parameter for the Gateway/IP-to-IP application or SBCProxyRegistrationTime parameter for the SBC application.</p>
<p>Web: Proxy Load Balancing Method EMS: Load Balancing</p>	<p>Enables the Proxy Load Balancing mechanism per Proxy Set ID.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Load Balancing is disabled (default)</li> <li><b>[1]</b> Round Robin</li> </ul>

Parameter	Description
Method CLI: control-network proxy-set > proxy- load-balancing- method <b>[ProxySet_ProxyLoadBalancingMethod]</b>	<ul style="list-style-type: none"> <li>▪ <b>[2] Random Weights</b></li> </ul> <p>When the Round Robin algorithm is used, a list of all possible Proxy IP addresses is compiled. This list includes all IP addresses per Proxy Set, after necessary DNS resolutions (including NAPTR and SRV, if configured). After this list is compiled, the Proxy Keep-Alive mechanism (according to parameters EnableProxyKeepAlive and ProxyKeepAliveTime) tags each entry as 'offline' or 'online'. Load balancing is only performed on Proxy servers that are tagged as 'online'.</p> <p>All outgoing messages are equally distributed across the list of IP addresses. REGISTER messages are also distributed unless a RegistrarIP is configured.</p> <p>The IP addresses list is refreshed according to ProxyIPListRefreshTime. If a change in the order of the entries in the list occurs, all load statistics are erased and balancing starts over again.</p> <p>When the Random Weights algorithm is used, the outgoing requests are not distributed equally among the Proxies. The weights are received from the DNS server by using SRV records. The device sends the requests in such a fashion that each Proxy receives a percentage of the requests according to its assigned weight. A single FQDN should be configured as a Proxy IP address. The Random Weights Load Balancing is not used in the following scenarios:</p> <ul style="list-style-type: none"> <li>▪ The Proxy Set includes more than one Proxy IP address.</li> <li>▪ The only Proxy defined is an IP address and not an FQDN.</li> <li>▪ SRV is not enabled (DNSQueryType).</li> <li>▪ The SRV response includes several records with a different Priority value.</li> </ul>
Web/EMS: Is Proxy Hot-Swap CLI: control-network proxy-set > is-proxy- hot-swap <b>[ProxySet_IsProxyHotSwap]</b>	<p>Enables the Proxy Hot-Swap redundancy mode.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] No (default)</b></li> <li>▪ <b>[1] Yes</b></li> </ul> <p>If Proxy Hot-Swap is enabled, the SIP INVITE/REGISTER message is initially sent to the first Proxy/Registrar server. If there is no response from the first Proxy/Registrar server after a specific number of retransmissions (configured by the parameter HotSwapRtx), the message is resent to the next redundant Proxy/Registrar server.</p>
Web/EMS: Redundancy Mode CLI: control-network proxy-set > proxy- redundancy-mode <b>[ProxySet_ProxyRedundancyMode]</b>	<p>Determines whether the device switches back to the primary Proxy after using a redundant Proxy.</p> <ul style="list-style-type: none"> <li>▪ <b>[-1] Not configured = (Default)</b> The global parameter, ProxyRedundancyMode applies.</li> <li>▪ <b>[0] Parking</b> = The device continues operating with a redundant (now active) Proxy until the next failure, after which it operates with the next redundant Proxy.</li> <li>▪ <b>[1] Homing</b> = The device always attempts to operate with the primary Proxy server (i.e., switches back to the primary Proxy whenever it's available).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To use the Proxy Redundancy mechanism, you need to enable the keep-alive with Proxy option, by setting the parameter EnableProxyKeepAlive to 1 or 2.</li> <li>▪ If this parameter is configured, then the global parameter is ignored.</li> </ul>
Web/EMS: SRD Index CLI: control-network proxy-set > srd-id	<p>Defines the SRD associated with the Proxy Set ID.</p> <p>The default is SRD 0.</p>

Parameter	Description
[ProxySet_ProxySet_SRD]	<b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>To configure SRDs, see Configuring SRD Table on page 199.</li> </ul>
Web/EMS: Classification Input CLI: control-network proxy-set > classification-input [ClassificationInput]	Defines how the device classifies an IP call to the Proxy Set. <ul style="list-style-type: none"> <li><b>[0]</b> Compare only IP = (Default) The call is classified to the Proxy Set according to its IP address only.</li> <li><b>[1]</b> Compare IP, port and transport type = The call is classified to the Proxy Set according to its IP address, port, and transport type.</li> </ul> <b>Note:</b> This parameter is applicable only if the IP Group table's parameter, 'Classify by Proxy Set' is set to Enable.

## 21.5 Associating WAN Interface with VoIP Traffic

If you are using the WAN interface, you need to associate it with VoIP traffic (i.e., SIP signaling and media interfaces). The available WAN interfaces depend on the hardware configuration and/or whether VLANs are configured for the WAN interface. If VLANs are configured, then you can select the WAN VLAN on which you want to run the SIP signaling and media interfaces.

Once this association is set, VoIP traffic is sent through the WAN and incoming traffic is identified as coming from the WAN. The device automatically configures the required port forwarding and static NAT rules.



**Note:** If you do not assign the WAN interface to SIP and media interfaces, then the WAN interface may not be used for VoIP traffic. In such cases, the VoIP traffic can be sent and received within the LAN or sent to the WAN through a third-party LAN router. If a third-party router is used as the interface to the WAN, then you need to configure NAT rules (in the NAT Translation table) to translate the VoIP LAN IP addresses (configured in the Multiple Interface table and associated with SIP and media interfaces) into global, public IP addresses.

### ➤ To assign a WAN interface to VoIP traffic:

1. Select the WAN interface:
  - a. Open the Multiple Interface Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**).

**Figure 21-4: Selecting WAN Interface for VoIP Traffic**

- b. From the 'WAN Interface Name' drop-down list, select the WAN interface for VoIP traffic.
  - c. Click **Done**, and then reset the device for your setting to take effect.

2. Assign the selected WAN interface to SIP signaling and RTP (media) interfaces in the SIP Interface and Media Realm tables, respectively. To denote the WAN interface, use the string value "WAN":
  - a. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SIP Interface Table**) and configure SIP interfaces on the WAN interface.

**Figure 21-5: Assigning SIP Interface to WAN**

SIP Interface Table							
Add +							
Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD	Message Policy
0	WAN	SBC	5060	5060	5061	1	None
1	Voice_Mng	SBC	5080	5080	5067	2	None

Page 1 of 1 Show 10 records per page View 1 - 2 of 2

- b. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Realm Configuration**) and configure media interfaces on the WAN interface.

**Figure 21-6: Assigning WAN Interface to Media Realm**

Media Realm Table			
Add			
Index	Media Realm Name	IPv4 Interface Name	IPv6 Interface Name
1	Media_1	Voice_Mng	None
2	Media_2	WAN	None

Page 1 of 1 Show 10 View 1 - 2 of 2

- c. Configure SRDs and associate them with these SIP signaling and media interfaces.
    - d. Configure other SIP settings as required.

## 22 SIP Definitions

This section describes configuration of SIP parameters.

### 22.1 Configuring SIP Parameters

Many of the stand-alone SIP parameters associated with various features can be configured in the following pages:

- **SIP General Parameters page:** Provides SIP parameters for configuring general SIP features. To access this page, use the following path: **Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**.
- **SIP Advanced Parameters page:** Provides SIP parameters for configuring advanced SIP features. To access this page, use the following path: **Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**.

For a description of these parameters, refer to the section corresponding to the feature or see 'Configuration Parameters Reference' on page [661](#).

### 22.2 Configuring Account Table

The Account Table page lets you define up to 32 Accounts per ("served") Trunk Group or source ("served") IP Group. Accounts are used to register and/or digest authenticate a Trunk Group or served IP Group, using a username and password, to a destination ("serving") IP Group. For example, the device can use the Account table to register an IP PBX, which is connected to the device, to an ITSP. The device sends the registration requests to the Proxy Set ID (see 'Configuring Proxy Sets Table' on page [213](#)) that is associated with the serving IP Group.

A Trunk Group or served IP Group can register to more than one serving IP Group (e.g., multiple ITSPs). This is done by configuring multiple entries in the Account table for the same Trunk Group or served IP Group, but with different serving IP Groups, user name/password, host name, and contact user values.

When using the Account table to register a Trunk Group, if all trunks belonging to the Trunk Group are down, the device un-registers the trunks. If any trunk belonging to the Trunk Group is returned to service, the device registers them again. This ensures, for example, that the Proxy does not send INVITEs to trunks that are out of service.

If registration to an IP Group fails for all accounts of a specific Trunk Group and if this Trunk Group includes all the channels in the Trunk Group, the Trunk Group is set to Out-Of-Service if the OOSOnRegistrationFail parameter is set to 1 (see 'Proxy & Registration Parameters' on page [222](#)).



**Notes:**

- For viewing Account registration status, see Viewing Endpoint Registration Status on page [595](#).
- The Account table can also be configured using the table ini file parameter, Account or CLI command, configure voip > sip-definition account.



➤ **To configure Accounts:**

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

<input type="text"/> <input type="button" value="Add"/> <input type="button" value="Compact"/> <input type="button" value="Delete"/> <input type="button" value="Apply"/>								
Index	Served Trunk Group	Served IP Group	Serving IP Group	Username	Password	Host Name	Register	ContactUser
1	1	3	1	isp-a	*	region-a	Yes	ITSPA-A
2	1	3	2	isp-b		region-b	Yes	ITSP-B

2. In the 'Add' field, enter the desired table row index, and then click **Add**. A new row appears.
3. Configure the Account parameters according to the table below.
4. Click the **Apply** button to save your changes.
5. To save the changes, see 'Saving Configuration' on page 532.
6. To perform registration, click the **Register** button; to unregister, click **Unregister**. The registration method for each Trunk Group is according to the setting of the 'Registration Mode' parameter in the Trunk Group Settings page.

#### Account Table Parameters Description

Parameter	Description
Served Trunk Group CLI: served-trunk-group <b>[Account_ServedTrunkGroup]</b>	Defines the Trunk Group ID that you want to register and/or authenticate to a destination IP Group (i.e., serving IP Group). <ul style="list-style-type: none"> <li>For Tel-to-IP calls, the Served Trunk Group is the source Trunk Group from where the call originated.</li> <li>For IP-to-Tel calls, the Served Trunk Group is the HuntTrunk Group ID to which the call is sent.</li> </ul> <b>Note:</b> This parameter is applicable only to the Gateway application.
Served IP Group CLI: served-ip-group <b>[Account_ServedIPGroup]</b>	Defines the Source IP Group (e.g., IP-PBX) for which registration and/or authentication is done. <b>Note:</b> This parameter is applicable only to the SBC and IP-to-IP applications (not Gateway application).
Serving IP Group CLI: serving-ip-group <b>[Account_ServingIPGroup]</b>	Defines the destination IP Group ID to where the SIP REGISTER requests, if enabled, are sent and authentication is done. The actual destination to where the REGISTER requests are sent is the IP address configured for the Proxy Set ID that is associated with the IP Group.           Registration occurs only if: <ul style="list-style-type: none"> <li><b>Gateway application only:</b> The 'Registration Mode' parameter is set to 'Per Account' in the Hunt Group Settings table (see Configuring Hunt Group Settings on page 291).</li> <li>The 'Register' parameter in the Account table is set to <b>Yes</b>.</li> </ul> For the Gateway and IP-to-IP applications: <ul style="list-style-type: none"> <li>For Tel-to-IP calls, the serving IP Group is the destination IP Group defined in the Trunk Group Settings table or Outbound IP Routing Table (see Configuring the Outbound IP Routing Table on page 321).</li> <li>For IP-to-Tel calls, the Serving IP Group is the 'Source IP Group ID' defined in the Inbound IP Routing Table (see Configuring the Inbound IP Routing Table on page 330).</li> </ul> <b>Note:</b> If no match is found in this table for incoming or outgoing calls, the username and password is taken from the following: <ul style="list-style-type: none"> <li>FXS interfaces: Authentication table (see Configuring Authentication)</li> <li>UserName and Password parameters on the Proxy &amp; Registration page.</li> </ul>



Parameter	Description
Username CLI: user-name [Account_Username]	Defines the digest MD5 Authentication user name. The valid value is a string of up to 50 characters.
Password CLI: password [Account_Password]	Defines the digest MD5 Authentication password. The valid value is a string of up to 50 characters. <b>Note:</b> After you click the <b>Apply</b> button, this password is displayed as an asterisk (*).
Host Name CLI: host-name [Account_HostName]	Defines the Address of Record (AOR) host name. It appears in REGISTER From/To headers as ContactUser@HostName. For successful registrations, this host name is also included in the INVITE request's From header URI. This parameter can be up to 49 characters. <b>Note:</b> If this parameter is not configured or if registration fails, the 'SIP Group Name' parameter configured in the IP Group table is used instead.
Register CLI: register [Account_Register]	Enables registration. <ul style="list-style-type: none"> <li>[0] No (Default)</li> <li>[1] Yes</li> </ul> <p>When enabled, the device sends REGISTER requests to the Serving IP Group. The host name (i.e., host name in SIP From/To headers) and Contact User (user in From/To and Contact headers) are taken from this table upon successful registration. See the example below:</p> <pre>REGISTER sip:xyz SIP/2.0 Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac1397582418 From: &lt;sip:ContactUser@HostName&gt;;tag=1c1397576231 To: &lt;sip: ContactUser@HostName &gt; Call-ID: 1397568957261200022256@10.33.37.78 CSeq: 1 REGISTER Contact: &lt;sip:ContactUser@10.33.37.78&gt;;expires=3600 Expires: 3600 User-Agent: Sip-Gateway/v.6.00A.008.002 Content-Length: 0</pre> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To activate registration, you also need to set the parameter 'Registration Mode' to 'Per Account' in the Trunk Group Settings table for the specific Trunk Group.</li> <li>The Trunk Group account registration is not affected by the parameter IsRegisterNeeded.</li> </ul>
Contact User CLI: contact-user [Account_ContactUser]	Defines the AOR user name. This appears in REGISTER From/To headers as ContactUser@HostName, and in INVITE/200 OK Contact headers as ContactUser@<device's IP address>. <b>Notes:</b> <ul style="list-style-type: none"> <li>If this parameter is not configured, the 'Contact User' parameter in the IP Group table is used instead.</li> <li>If registration fails, then the user part in the INVITE Contact header contains the source party number.</li> </ul>
Application Type CLI: application-type [Account_ApplicationType]	Defines the application type: <ul style="list-style-type: none"> <li>[0] GW/IP2IP = (Default) Gateway and IP-to-IP application.</li> <li>[2] SBC = SBC application.</li> </ul>

## 22.3 Configuring Proxy and Registration Parameters

The Proxy & Registration page [allows](#) you to configure the Proxy server and registration parameters. For a description of the parameters appearing on this page, see 'Configuration Parameters Reference' on page [661](#).



**Note:** To view the registration status of endpoints with a SIP Registrar/Proxy server, see Viewing Endpoint Registration Status on page [595](#).

➤ **To configure the Proxy and registration parameters:**

1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Proxy & Registration**).

**Figure 22-1: Proxy & Registration Page**

Use Default Proxy	Yes
Proxy Set Table	
Proxy Name	
Redundancy Mode	Homing
Proxy IP List Refresh Time	60
Enable Fallback to Routing Table	Disable
Prefer Routing Table	No
Use Routing Table for Host Names and Profiles	Disable
Always Use Proxy	Disable
Redundant Routing Mode	Disable
SIP ReRouting Mode	Standard Mode
Enable Registration	Disable
Registration Time	180
Re-registration Timing [%]	50
Registration Retry Time	30
Registration Time Threshold	0
Re-register On INVITE Failure	Disable
ReRegister On Connection Failure	Disable
Gateway Name	ipcs20.callbox.kt.com
Gateway Registration Name	
DNS Query Type	A-Record
Proxy DNS Query Type	A-Record
Subscription Mode	Per Endpoint
Number of RTX Before Hot-Swap	3
Use Gateway Name for OPTIONS	No
User Name	
Password	Default_Passwd
Cnonce	Default_Cnonce
Registration Mode	Per FXS
Set Out-Of-Service On Registration Failure	Disable
Challenge Caching Mode	None
Mutual Authentication Mode	Optional


2. Configure the parameters as required.
3. Click **Submit** to apply your changes.

➤ **To register or un-register the device to a Proxy/Registrar:**

- Click the **Register** button to register.
- Click **Un-Register** button to un-register.

Instead of registering the entire device, you can register specific entities as listed below by using the **Register** button located on the page in which these entities are configured:

- FXS/FXO endpoints, BRI endpoints, Trunk Groups - Trunk Group Table page (see [Configuring Trunk Group Table](#) on page 289)
- Accounts - Account table (see 'Configuring Account Table' on page 219)

Click the **Proxy Set Table**  button to Open the Proxy Sets Table page to configure groups of proxy addresses. Alternatively, you can open this page from the **Proxy Sets Table** page item (see 'Configuring Proxy Sets Table' on page 213 for a description of this page).

### 22.3.1 SIP Message Authentication Example

The device supports basic and digest (MD5) authentication types, according to SIP RFC 3261 standard. A proxy server might require authentication before forwarding an INVITE message. A Registrar/Proxy server may also require authentication for client registration. A proxy replies to an unauthenticated INVITE with a 407 Proxy Authorization Required response, containing a Proxy-Authenticate header with the form of the challenge. After sending an ACK for the 407, the user agent can then re-send the INVITE with a Proxy-Authorization header containing the credentials.

User agents, Redirect or Registrar servers typically use the SIP 401 Unauthorized response to challenge authentication containing a WWW-Authenticate header, and expect the re-INVITE to contain an Authorization header.

The following example shows the Digest Authentication procedure, including computation of user agent credentials:

1. The REGISTER request is sent to a Registrar/Proxy server for registration:

```
REGISTER sip:10.2.2.222 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.200
From: <sip:122@10.1.1.200>;tag=1c17940
To: <sip:122@10.1.1.200>
Call-ID: 634293194@10.1.1.200
User-Agent: Sip-Gateway/Mediant 800 MSBR/v.6.60.010.006
CSeq: 1 REGISTER
Contact: sip:122@10.1.1.200:
Expires:3600
```

2. Upon receipt of this request, the Registrar/Proxy returns a 401 Unauthorized response:

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 10.2.1.200
From: <sip:122@10.2.2.222 >;tag=1c17940
To: <sip:122@10.2.2.222 >
Call-ID: 634293194@10.1.1.200
Cseq: 1 REGISTER
Date: Mon, 30 Jul 2012 15:33:54 GMT
Server: Columbia-SIP-Server/1.17
Content-Length: 0
WWW-Authenticate: Digest realm="audiocodes.com",
nonce="11432d6bce58ddf02e3b5e1c77c010d2",
stale=FALSE,
algorithm=MD5
```

3. According to the sub-header present in the WWW-Authenticate header, the correct REGISTER request is created.
4. Since the algorithm is MD5:
  - The username is equal to the endpoint phone number "122".
  - The realm return by the proxy is "audiocodes.com".
  - The password from the *ini* file is "AudioCodes".
  - The equation to be evaluated is "122:audiocodes.com:AudioCodes". According to the RFC, this part is called A1.
  - The MD5 algorithm is run on this equation and stored for future usage.
  - The result is "a8f17d4b41ab8dab6c95d3c14e34a9e1".
5. The par called A2 needs to be evaluated:
  - The method type is "REGISTER".
  - Using SIP protocol "sip".
  - Proxy IP from *ini* file is "10.2.2.222".

- The equation to be evaluated is "REGISTER:sip:10.2.2.222".
- The MD5 algorithm is run on this equation and stored for future usage.
- The result is "a9a031cfdccb10d91c8e7b4926086f7e".

**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 800 MSBR/v.6.60.010.006
CSeq: 1 REGISTER
Contact: sip:122@10.1.1.200:
Expires:3600
Authorization: Digest, username: 122,
realm="audiocodes.com",
nonce="11432d6bce58ddf02e3b5e1c77c010d2",
uri="10.2.2.222",
response="b9c45d0234a5abf5ddf5c704029b38cf"
```

**7. Upon receiving this request and if accepted by the Proxy, the Proxy returns a 200 OK response, completing the registration transaction:**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c23940
To: <sip: 122@10.1.1.200>
Call-ID: 654982194@10.1.1.200
Cseq: 1 REGISTER
Date: Thu, 26 Jul 2012 09:34:42 GMT
Server: Columbia-SIP-Server/1.17
Content-Length: 0
Contact: <sip:122@10.1.1.200>; expires="Thu, 26 Jul 2012
10:34:42 GMT"; action=proxy; q=1.00
Contact: <122@10.1.1.200:>; expires="Tue, 19 Jan 2038 03:14:07
GMT"; action=proxy; q=0.00
Expires: Thu, 26 Jul 2012 10:34:42 GMT
```

## 22.4 Configuring SIP Message Manipulation

The Message Manipulations page allows you to define up to 100 SIP message manipulation rules. Each manipulation rule can be assigned any Manipulation Set ID (0 to 19), enabling you to create groups (sets) of manipulation rules whereby rules of a group are configured with the same Manipulation Set ID number. To use these Manipulation Sets, you need to assign them to IP Groups in the IP Group table (see 'Configuring IP Groups' on page 204) where they can be applied to inbound and/or outbound SIP messages.

SIP message manipulation enables the normalization of SIP messaging fields between communicating network segments. For example, it allows service providers to design their own policies on the SIP messaging fields that must be present before a SIP call enters their network. Similarly, enterprises and small businesses may have policies for the information that can enter or leave their networks for policy or security reasons from a service provider. The manipulations can also be implemented to resolve incompatibilities between SIP devices inside the enterprise network.

SIP message manipulation supports the following:

- Addition of new headers.
- Removal of headers ("Black list").
- Modification of header components - value, header value (e.g., URI value of the P-Asserted-Identity header can be copied to the From header), call's parameter values.
- Deletion of SIP body (e.g., if a message body isn't supported at the destination network this body is removed).
- Translating one SIP response code to another.
- Topology hiding (generally present in SIP headers such as Via, Record Route, Route and Service-Route).
- Configurable identity hiding (information related to identity of subscribers for example, P-Asserted-Identity, Referred-By, Identity and Identity-Info).
- Apply conditions per rule - the condition can be on parts of the message or call's parameters.
- Multiple manipulation rules on the same SIP message.

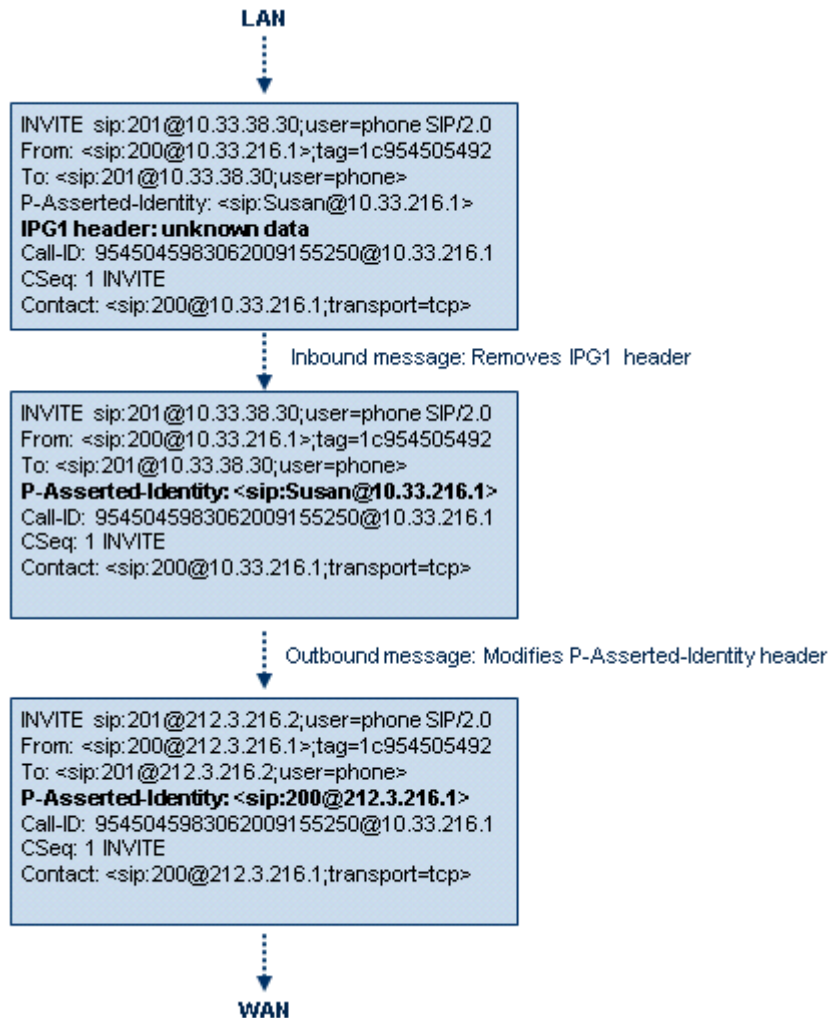
The manipulation is performed on SIP messages according to the Classification table (source/destination of username/host prefixes, and source IP address). The manipulation can be performed on message type (Method, Request/Response, and Response type) and multiple manipulation rules can be configured for the same SIP message.

For the Gateway / IP-to-IP application, manipulation rules can be assigned as follows:

- Manipulating inbound SIP INVITE messages: The Manipulation Set ID is selected using the "global" parameter, GWInboundManipulationSet. If this parameter is not configured, then no manipulation is done.
- Manipulating outbound SIP INVITE messages: The Manipulation Set ID is selected using the following logic:
  - a. According to the settings of the 'Outbound Message Manipulation Set' parameter configured for the destination IP Group (in the IP Group table). In other words, manipulation can be done per destination IP Group. If this parameter is not configured, see below.
  - b. According to the settings of the "global" parameter, GWOOutboundManipulationSet. If this parameter is not configured, no manipulation is done.

The figure below illustrates a SIP message manipulation example:

**Figure 22-2: SIP Header Manipulation Example**



**Notes:**

- For a detailed description of the syntax for configuring SIP message manipulation rules, refer to *SIP Message Manipulations Quick Reference Guide*.
- For the IP-to-IP application, the outgoing message is re-created and thus, SIP headers that are not relevant to the outgoing SIP session (e.g., Referred-By) are not included in the outgoing message. Therefore, if required, manipulations on such headers should be handled in inbound manipulation.
- The values entered in the table are not case-sensitive.
- For the SBC application, SIP message manipulation is done only after the Classification, inbound/outbound number manipulations, and routing processes.
- Each message can be manipulated twice - on the source leg and on the destination leg (i.e., source and destination IP Groups).
- Unknown SIP parts can only be added or removed.
- SIP manipulations do not allow you to remove or add mandatory SIP



headers. They can only be modified and only on requests that initiate new dialogs. Mandatory SIP headers include To, From, Via, CSeq, Call-Id, and Max-Forwards.

- The Message Manipulations table can also be configured using the table *ini* file parameter, MessageManipulations or CLI command, configure voip > sbc manipulations message-manipulations.

➤ **To configure SIP message manipulation rules:**

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Click the **Add** button; the following dialog box appears:

**Figure 22-3: Message Manipulations Table - Add Record Dialog Box**

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

- Index:** Text input field with value 0.
- Manipulation Set ID:** Text input field with value 0.
- Message Type:** Text input field.
- Condition:** Text input field.
- Action Subject:** Text input field.
- Action Type:** Dropdown menu with "Add" selected.
- Action Value:** Text input field.
- Row Role:** Dropdown menu with "Use Current Condition" selected.
- Buttons:** "Submit" and "Cancel" buttons at the bottom right.

3. Configure the SIP message manipulation rule as required. See the table below for a description of each parameter.
4. Click **Submit** to apply your changes.

The figure below displays an example of configured message manipulation rules:

- Index 0 - adds the suffix ".com" to the host part of the To header.
- Index 1 - changes the user part of the From header to the user part of the P-Asserted-ID.
- Index 2 - changes the user part of the SIP From header to "200".
- Index 3 - if the user part of the From header equals "unknown", then it is changed according to the srcIPGroup call's parameter.
- Index 4 - removes the Priority header from an incoming INVITE message.

**Figure 22-4: Message Manipulations Page**

Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value
0	0	invite.response.200		header.to.url.user	Add Prefix	'.com'
1	1	invite.response.200		header.from.url.user	Modify	header.p-asserted-id.url.user
2	2	invite.request		header.from.url.user	Modify	'200'
3	3	invite.request	header.from.url.user=='Unkn	header.from.url.user	Modify	param.ipq.src.user
4	4	invite.request		header.priority	Remove	



### Message Manipulations Parameters

Parameter	Description
Index [MessageManipulations_Index]	Defines the table row index for the rule. The valid value is 0 to 99. The default is 0. <b>Note:</b> Each rule must be configured with a unique index.
Manipulation Set ID CLI: 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 Group table) for inbound and/or outbound messages. The valid value is 0 to 19. The default is 0.
<b>Matching Characteristics</b>	
Message Type CLI: message-type [MessageManipulations_MessageType]	Defines the SIP message type that you want to manipulate. The valid value is a string denoting the SIP message. For example: <ul style="list-style-type: none"> <li>Empty = rule applies to all messages</li> <li>Invite = rule applies to all INVITE requests and responses</li> <li>Invite.Request = rule applies to INVITE requests</li> <li>Invite.Response = rule applies to INVITE responses</li> <li>subscribe.response.2xx = rule applies to SUBSCRIBE confirmation responses</li> </ul> <b>Note:</b> Currently, SIP 100 Trying messages cannot be manipulated.
Condition CLI: condition [MessageManipulations_Condition]	Defines the condition that must exist for the rule to apply. The valid value is a string. For example: <ul style="list-style-type: none"> <li>header.from.url.user== '100' (indicates that the user part of the From header must have the value "100")</li> <li>header.contact.param.expires &gt; '3600'</li> <li>header.to.url.host contains 'domain'</li> <li>param.call.dst.user != '100'</li> </ul>
<b>Operation</b>	
Action Subject CLI: action-subject [MessageManipulations_ActionSubject]	Defines the SIP header upon which the manipulation is performed.
Action Type CLI: action-type [MessageManipulations_ActionType]	Defines the type of manipulation. <ul style="list-style-type: none"> <li><b>[0]</b> Add (default) = adds new header/param/body (header or parameter elements).</li> <li><b>[1]</b> Remove = removes header/param/body (header or parameter elements).</li> <li><b>[2]</b> Modify = sets element to the new value (all element types).</li> <li><b>[3]</b> Add Prefix = adds value at the beginning of the string (string element only).</li> <li><b>[4]</b> Add Suffix = adds value at the end of the string (string element only).</li> <li><b>[5]</b> Remove Suffix = removes value from the end of the string (string element only).</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li><b>[6] Remove Prefix</b> = removes value from the beginning of the string (string element only).</li> </ul>
Action Value CLI: action-value <b>[MessageManipulations_ActionValue]</b>	Defines a value (string) that you want to use in the manipulation. The syntax is as follows: <ul style="list-style-type: none"> <li>string/&lt;message-element&gt;/&lt;call-param&gt; +</li> <li>string/&lt;message-element&gt;/&lt;call-param&gt;</li> </ul> For example: <ul style="list-style-type: none"> <li>'itsp.com'</li> <li>header.from.url.user</li> <li>param.call.dst.user</li> <li>param.call.dst.host + '.com'</li> <li>param.call.src.user + '&lt;' + header.from.url.user + '@' + header.p-asserted-id.url.host + '&gt;'</li> </ul> <b>Note:</b> Only single quotation marks must be used.
Row Role CLI: row-role <b>[MessageManipulations_RowRole]</b>	Determines which condition must be used for the rule of this table row. <ul style="list-style-type: none"> <li><b>[0] Use Current Condition</b> = The condition entered in this row must be matched in order to perform the defined action (default).</li> <li><b>[1] Use Previous Condition</b> = The condition of the rule configured directly above this row must be used in order to perform the defined action. This option allows you to configure multiple actions for the same condition.</li> </ul> <b>Note:</b> When multiple manipulations rules apply to the same header, the next rule applies to the result string of the previous rule.

## 22.5 Configuring SIP Message Policy Rules

You can configure SIP message policy rules for blocking (blacklist) unwanted incoming SIP messages or allowing (whitelist) receipt of desired messages. This feature allows you to define legal and illegal characteristics of a SIP message. Message policies can be applied globally (default) or per signaling domain by assigning it to a SIP interface in the SIP Interface table (see 'Configuring SIP Interface Table' on page 201).

This feature is helpful against VoIP fuzzing (also known as robustness testing), which sends different types of packets to its "victims" for finding bugs and vulnerabilities. For example, the attacker might try sending a SIP message containing either an over-sized parameter or too many occurrences of a parameter.

Each message policy rule can be configured with the following:

- Maximum message length
- Maximum SIP header length
- Maximum message body length
- Maximum number of headers
- Maximum number of bodies
- Option to send 400 "Bad Request" response if message request is rejected
- Blacklist and whitelist for defined SIP methods (e.g., INVITE)
- Blacklist and whitelist for defined SIP bodies



**Note:** The Message Policy table can also be configured using the table ini file parameter, MessagePolicy or the CLI command, configure voip > sbc message-policy.

➤ **To configure SIP message policy rules:**

1. Open the Message Policy Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Policy Table**).
2. Click the **Add** button; the Add Record dialog box appears:

**Figure 22-5: Message Policy Table - Add Record Dialog Box**

The policy defined above limits SIP messages to 32,768 characters, headers to 256 characters, bodies to 512 characters, number of headers to 16, and only permits two bodies. Invalid requests are rejected. Only INVITE and BYE requests are permitted and there are no restrictions on bodies.

3. Configure the SIP message policy rule as required. See the table below for a description of each parameter.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 532.

**SIP Message Policy Parameters**

Parameter	Description
Index [MessagePolicy_Index]	Defines the table index entry.
Max Message Length CLI: 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.
Max Header Length CLI: max-header-length [MessagePolicy_MaxHeaderLength]	Defines the maximum SIP header length. The valid value is up to 512 characters. The default is 512.

Parameter	Description
Max Body Length CLI: max-body-length <b>[MessagePolicy_MaxBodyLength]</b>	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 CLI: max-num-headers <b>[MessagePolicy_MaxNumHeaders]</b>	Defines the maximum number of SIP headers. The valid value is any number up to 32. The default is 32. <b>Note:</b> The device supports up to 20 SIP Record-Route headers that can be received in a SIP INVITE request or 200 OK response. If it receives more than this, it responds with a SIP 513 'Message Too Large' response.
Max Num Bodies CLI: max-num-bodies <b>[MessagePolicy_MaxNumBodies]</b>	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.
Send Rejection CLI: send-rejection <b>[MessagePolicy_SendRejection]</b>	Determines whether the device sends a 400 "Bad Request" response if a message request is rejected. <ul style="list-style-type: none"> <li><b>[0]</b> Policy Reject = (Default) If the message is a request, then the device sends a response to reject the request.</li> <li><b>[1]</b> Policy Drop = The device ignores the message without sending any response.</li> </ul>
Method List CLI: method-list <b>[MessagePolicy_MethodList]</b>	Defines the SIP methods (e.g., INVITE\BYE) to which the rule applies. The syntax for entering the methods is as follows: <ul style="list-style-type: none"> <li>Methods must be separated by a backslash (\).</li> <li>The entered value is not case sensitive.</li> </ul>
Method List Type CLI: method-list-type <b>[MessagePolicy_MethodListType]</b>	Determines the policy for the SIP methods. <ul style="list-style-type: none"> <li><b>[0]</b> Policy Blacklist = The specified methods (in the 'Method List' field) are rejected by the policy.</li> <li><b>[1]</b> Policy Whitelist = (Default) The specified methods (in the 'Method List' field) are allowed by the policy.</li> </ul>
Body List CLI: body-list <b>[MessagePolicy_BodyList]</b>	Defines the SIP body (i.e., value of the Content-Type header) to which the rule applies.
Body List Type CLI: body-list-type <b>[MessagePolicy_BodyListType]</b>	Determines the policy for the defined SIP body. <ul style="list-style-type: none"> <li><b>[0]</b> Policy Blacklist = The specified SIP body (in the 'Body List' field) is rejected by the policy.</li> <li><b>[1]</b> Policy Whitelist = (Default) The specified SIP body (in the 'Body List' field) is allowed by the policy.</li> </ul>

## 23 Coders and Profiles

This section describes configuration of the coders and SIP profiles parameters.

### 23.1 Configuring Coders

The Coders page allows you to configure up to 10 voice coders for the device. Each coder can be configured with packetization time (ptime), bit rate, payload type, and silence suppression. The first coder configured in the table 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 table, and so on.



#### Notes:

- A specific coder can only be configured once in the table.
- If packetization time and/or rate are not specified, the default value is applied.
- Only the packetization time of the first coder in the coder list is declared in INVITE/200 OK SDP, even if multiple coders are defined.
- 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 several fields is hard-coded according to common standards (e.g., payload type of G.711 U-law is always 0). Other values can be set dynamically. If no value is specified for a dynamic field, a default value is assigned. If a value is specified for a hard-coded field, the value is ignored.
- If silence suppression is not configured for a coder, the settings of the EnableSilenceCompression parameter is used.
- The G.722 coder provides Packet Loss Concealment (PLC) capabilities, ensuring higher voice quality.
- For G.729, it's also possible to select silence suppression without adaptations.
- If G.729 is selected and silence suppression is disabled, the device includes 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is enabled or set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception to this logic is when the remote gateway is a Cisco device (IsCiscoSCEMode).
- For defining groups of coders, which can be assigned to Tel and IP Profiles, see 'Configuring Coder Groups' on page 236.
- For information on V.152 and implementation of T.38 and VBD coders, see 'Supporting V.152 Implementation' on page 160.
- The Coders table can also be configured using the table *ini* file parameter, CodersGroup or CLI command, configure voip > coders-and-profiles coders-group-<index>.

➤ **To configure the device's coders:**

1. Open the Coders page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** submenu > **Coders**).

**Figure 23-1: Coders Table Page**

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.723.1	30	5.3	4	Disabled

2. From the 'Coder Name' drop-down list, select the required coder.
3. From the 'Packetization Time' drop-down list, select the packetization time (in msec) for the selected coder. The packetization time determines how many coder payloads are combined into a single RTP packet.
4. From the 'Rate' drop-down list, select the bit rate (in kbps) for the selected coder.
5. In the 'Payload Type' field, if the payload type (i.e., format of the RTP payload) for the selected coder is dynamic, enter a value from 0 to 120 (payload types of 'well-known' coders cannot be modified).
6. From the 'Silence Suppression' drop-down list, enable or disable the silence suppression option for the selected coder.
7. Repeat steps 2 through 6 for the next optional coders.
8. Click **Submit**.
9. To save the changes to flash memory, see 'Saving Configuration' on page 532.

The table below lists the supported coders:

**Supported Coders**

Coder Name	Packetization Time (msec)	Rate (kbps)	Payload Type	Silence Suppression
G.711 A-law [g711Alaw64k]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	64	8	<ul style="list-style-type: none"> <li>▪ [0] Disable</li> <li>▪ [1] Enable</li> </ul>
G.711 U-law [g711Ulaw64k]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	64	0	<ul style="list-style-type: none"> <li>▪ [0] Disable</li> <li>▪ [1] Enable</li> </ul>
G.711A-law_VBD [g711AlawVbd]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	64	Dynamic (0-127) Default is 180	N/A
G.711U-law_VBD [g711UlawVbd]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	64	Dynamic (0-127) Default is 120	N/A
G.722 [g722]	20 (default), 40, 60, 80, 100, 120	64 (default)	9	N/A

Coder Name	Packetization Time (msec)	Rate (kbps)	Payload Type	Silence Suppression
G.723.1 [g7231]	30 (default), 60, 90, 120, 150	<ul style="list-style-type: none"> <li>▪ [0] 5.3 (default)</li> <li>▪ [1] 6.3</li> </ul>	4	<ul style="list-style-type: none"> <li>▪ [0] Disable</li> <li>▪ [1] Enable</li> </ul>
G.726 [g726]	10, 20 (default), 30, 40, 50, 60, 80	<ul style="list-style-type: none"> <li>▪ [0] 16</li> <li>▪ [1] 24</li> <li>▪ [2] 32 (default)</li> <li>▪ [3] 40</li> </ul>	Dynamic (0-127) Default is 23	<ul style="list-style-type: none"> <li>▪ [0] Disable</li> <li>▪ [1] Enable</li> </ul>
G.729 [g729]	10, 20 (default), 30, 40, 50, 60, 80, 100	8	18	<ul style="list-style-type: none"> <li>▪ [0] Disable</li> <li>▪ [1] Enable</li> <li>▪ [2] Enable w/o Adaptations</li> </ul>
AMR [Amr]	20 (default)	<ul style="list-style-type: none"> <li>▪ [0] 4.75</li> <li>▪ [1] 5.15</li> <li>▪ [2] 5.90</li> <li>▪ [3] 6.70</li> <li>▪ [4] 7.40</li> <li>▪ [5] 7.95</li> <li>▪ [6] 10.2</li> <li>▪ [7] 12.2 (default)</li> </ul>	Dynamic (0-127)	<ul style="list-style-type: none"> <li>▪ [0] Disable</li> <li>▪ [1] Enable</li> </ul>
AMR-WB [Amr-WB]	20 (default)	<ul style="list-style-type: none"> <li>▪ [0] 6.6</li> <li>▪ [1] 8.85</li> <li>▪ [2] 12.65</li> <li>▪ [3] 14.25</li> <li>▪ [4] 15.85</li> <li>▪ [5] 18.25</li> <li>▪ [6] 19.85</li> <li>▪ [7] 23.05</li> <li>▪ [8] 23.85 (default)</li> </ul>	Dynamic (0-127)	<ul style="list-style-type: none"> <li>▪ [0] Disable</li> <li>▪ [1] Enable</li> </ul>
silk-nb [Silk-8KHz]	20 (default), 40, 60, 80, and 100	8	Dynamic (default is 76)	N/A
silk-wb [Silk-16KHz]	20 (default), 40, 60, 80, and 100	16	Dynamic (default is 77)	N/A
T.38 [t38fax]	N/A	N/A	N/A	N/A
T.38 Version 3 [t38fax]	-	-	-	-

## 23.2 Configuring Coder Groups

The Coder Group Settings page allows you to define up to 10 groups of coders (termed *Coder Groups*). For each Coder Group, you can define up to 10 coders configured with packetization time (ptime), rate, payload type, and silence suppression. The first coder in the Coder Group table 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, and so on.

Coder Groups can be used as follows:

- Assigned to Tel Profiles in the Tel Profiles table (see Configuring Tel Profiles on page 237). This is applicable only to the GW/IP-to-IP application.
- Assigned to IP Profiles in the IP Profiles table (see 'Configuring IP Profiles' on page 239). In this setup, they can be used as Extension coders and Allowed coders for the SBC application.



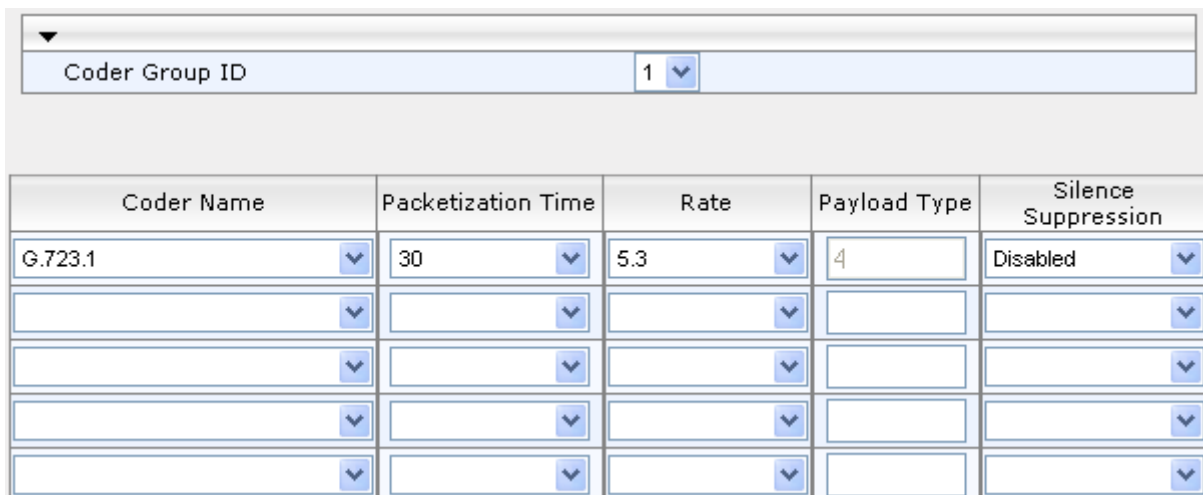
### Notes:

- A specific coder can be selected only once per Coder Group.
- For a list of supported coders, see 'Configuring Coders' on page 233.
- The Coder Group Settings table can also be configured using the table *ini* file parameter, CodersGroup or CLI command, configure voip > coders-and-profiles coders-group-<index>.

### ➤ To configure Coder Groups:

1. Open the Coder Group Settings page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** submenu > **Coders Group Settings**).

**Figure 23-2: Coder Group Settings Page**



Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.723.1	30	5.3	4	Disabled

2. From the 'Coder Group ID' drop-down list, select a Coder Group ID.
3. From the 'Coder Name' drop-down list, select the first coder for the Coder Group.
4. From the 'Packetization Time' drop-down list, select the packetization time (in msec) for the coder. The packetization time determines how many coder payloads are combined into a single RTP packet.
5. From the 'Rate' drop-down list, select the bit rate (in kbps) for the coder you selected.
6. In the 'Payload Type' field, if the payload type (i.e., format of the RTP payload) for the coder you selected is dynamic, enter a value from 0 to 120 (payload types of common coders cannot be modified).



7. From the 'Silence Suppression' drop-down list, enable or disable the silence suppression option for the coder you selected.
8. Repeat steps 3 through 7 for the next coders (optional).
9. Repeat steps 2 through 8 for the next coder group (optional).
10. Click **Submit** to apply your changes.

## 23.3 Configuring Tel Profile

The Tel Profile Settings table allows you to define up to nine configuration profiles for Tel calls. These profiles are termed *Tel Profiles*. The Tel Profile Settings table contains a list of parameters, which can also be configured globally for all calls using their corresponding "global" parameters. The only difference between the Tel Profile parameters and the global parameters regarding description may be their default values.

Tel Profiles provide high-level adaptation when the device interworks between different equipment and protocols (at both the Tel and IP sides), each of which may require different handling by the device. Once configured, Tel Profiles can be assigned to specific channels (trunks). Therefore, Tel Profiles enable you to assign special configuration settings for device handling of specific calls. For example, if specific channels require the use of the G.711 coder, you can configure a Tel Profile with this coder and assign it to these channels. Tel Profiles are assigned to channels in the Trunk Group Table (see Configuring the Trunk Group Table on page 289)).

The procedure below describes how to configure Tel Profiles using the Web interface.



**Note:** Tel Profiles can also be configured using the table *ini* file parameter, TelProfile (see 'Configuration Parameters Reference' on page 661) or CLI command, configure voip/coders-and-profiles tel-profile.

➤ **To configure Tel Profiles:**

1. Open the Tel Profile Settings page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** submenu > **Tel Profile Settings**).

Profile ID	1
Profile Name	mike
<b>Profile Parameters</b>	
Profile Preference	1
Fax Signaling Method	No Fax
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
Voice Volume (-32 to 31 dB)	0
DTMF Volume (-31 to 0 dB)	-11
Input Gain (-32 to 31 dB)	0
Enable Digit Delivery	Disable
Enable Polarity Reversal	Enable
Enable Current Disconnect	Disable
MWI Analog Lamp	Disable
MWI Display	Disable
Dial Plan Index	-1
Echo Canceler	Enable
Flash Hook Period	700
Enable Early Media	Disable
Progress Indicator to IP	Not Configured
Enable DID Wink	Disable
Dialing Mode	Two Stages
Enable Voice Mail Delay	Enable
Disconnect Call on Detection of Busy Tone	Enable
Time For Reorder Tone [sec]	255
Enable 911 PSAP	Disable
Enable AGC	Disable
EC NLP Mode	Adaptive NLP
Swap Tel To IP Phone Numbers	Disable
<b>Coder Group</b>	
Coder Group	Default Coder Group

2. From the 'Profile ID' drop-down list, select the Tel Profile index.
3. In the 'Profile Name' field, enter an arbitrary name that enables you to easily identify the Tel Profile.
4. From the 'Profile Preference' drop-down list, select the priority of the Tel Profile, where **1** is the lowest priority and **20** the highest. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk in the description of the parameter TelProfile) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.  
**Note:** If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used. The order of the coders is determined by the

preference.

5. Configure the parameters as required. For a description of each parameter, refer to the corresponding "global" parameter.
6. Click **Submit** to apply your changes.

## 23.4 Configuring IP Profiles

The IP Profile Settings table allows you to define up to nine *IP Profiles*. An IP Profile is a set of special call configuration behaviors relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder used) applied to specific IP calls (inbound and/or outbound). Therefore, IP Profiles provide high-level adaptation when the device interworks between different IP entities (for Tel and IP sides), each of which may require different handling by the device. For example, if a specific IP entity uses the G.711 coder only, you can configure an IP Profile with G.711 for this IP entity.

Many of the parameters in the IP Profile Settings table have a corresponding "global" parameter. If an IP Profile is not associated with specific calls, the settings of the global parameters are applied to these calls.

IP Profiles can be assigned to the following configuration elements:

- IP Groups - see Configuring IP Groups on page [204](#)
- Outbound IP routing rules - see Configuring Outbound IP Routing Table on page [321](#)
- Inbound IP routing rules - see Configuring Inbound IP Routing Table on page [330](#)

The device selects the IP Profile as follows:

- If different IP Profiles (not default) are assigned to the same specific calls in all these tables, the device uses the IP Profile that has the highest preference level (as set in the 'Profile Preference' field). If they have the same preference level, the device uses the IP Profile assigned in the IP Group table.
- If different IP Profiles are assigned to these tables and one table is set to the default IP Profile, the device uses the IP Profile that is not the default.

### Notes:

- IP Profiles can also be implemented when using a Proxy server (when the AlwaysUseRouteTable parameter is set to 1).
- RxDTMFOption configures the received DTMF negotiation method: [-1] not configured, use the global parameter; [0] don't declare RFC 2833; [1] declare RFC 2833 payload type is SDP.
- You can also configure IP Profiles using the table ini file parameter, IPProfile (see Configuration Parameters Reference on page [661](#)) or the CLI command, configure voip > coders-and-profiles ip-profile.

➤ **To configure IP Profiles:**

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** submenu > **IP Profile Settings**).

Profile ID	1
Profile Name	

▲ Common Parameters

▲ Gateway Parameters

▼ SBC

Transcoding Mode	Force
Extension Coders Group ID	None
Allowed Coders Group ID	None
Allowed Coders Mode	Restriction
Diversion Mode	Don't Care
History Info Mode	Don't Care
Media Security Behavior	As Is
RFC 2833 Behavior	As Is
Alternative DTMF Method	Don't Care
P-Asserted-Identity	Don't Care
SBC Fax Coders Group ID	None
SBC Fax Behavior	0
SBC Fax Offer Mode	0
SBC Fax Answer Mode	1
SBC Session Expires Mode	Transparent
SBC Remote Early Media RTP	Immediate
SBC Remote Can Play Ringback	Yes
SBC Remote Supports RFC 3960	Not Supported
SBC Multiple 18x Support	supported
SBC Early Media Response Type	Transparent
SBC Remote Update Support	Supported
SBC Remote Re-Invite Support	Supported
SBC Remote Refer Behavior	Transparent
SBC Remote Early Media Support	supported
SBC Remote 3xx Behavior	Transparent
SBC Remote Delayed Offer Support	Supported
SBC PRACK Mode	Transparent
SBC Enforce MKI Size	do-not-enforce
SBC User Registration Time	60
SBC Remote Hold Format	transparent

2. From the 'Profile ID' drop-down list, select the IP Profile index.
3. In the 'Profile Name' field, enter an arbitrary name that allows you to easily identify the IP Profile.
4. From the 'Profile Preference' drop-down list, select the priority of the IP Profile, where '1' is the lowest priority and '20' is the highest. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.  
**Note:** If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used. The order of the coders is determined by the preference.
5. Configure the parameters as required.
6. Click **Submit** to apply your changes.

Table 23-1: IP Profile Parameters Description

Parameter	Description
Web: Profile ID <b>[IpProfile_Index]</b>	Defines a unique index number for the IP Profile.
Web: Profile Name <b>[IpProfile_ProfileName]</b>	(Optional) Defines a descriptive name for the IP Profile.
<b>Common Parameters</b>	
Web: RTP IP DiffServ <b>[IpProfile_IPDiffServ]</b>	For a description, see the global parameter PremiumServiceClassMediaDiffServ.
Web: Signaling DiffServ <b>[IpProfile_SigIPDiffServ]</b>	For a description, see the global parameter PremiumServiceClassControlDiffServ.
Web: Disconnect on Broken Connection <b>[IpProfile_DisconnectOnBrokenConnection]</b>	For a description, see the global parameter DisconnectOnBrokenConnection.
Web: Media IP Version Preference <b>[IpProfile_MediaIPVersionPreference]</b>	For a description, see the global parameter MediaIPVersionPreference.
Web: Dynamic Jitter Buffer Minimum Delay <b>[IpProfile_JitterBufMinDelay]</b>	For a description, see the global parameter DJBufMinDelay.
Web: Dynamic Jitter Buffer Optimization Factor <b>[IpProfile_JitterBufOptFactor]</b>	For a description, see the global parameter DJBufOptFactor.
Web: RTP Redundancy Depth <b>[IpProfile_RTPRedundancyDepth]</b>	For a description, see the global parameter RTPRedundancyDepth.
Web: Echo Canceled <b>[IpProfile_EnableEchoCanceller]</b>	For a description, see the global parameter EnableEchoCanceller.
Web: Input Gain <b>[IpProfile_InputGain]</b>	For a description, see the global parameter InputGain.
Web: Voice Volume <b>[IpProfile_VoiceVolume]</b>	For a description, see the global parameter VoiceVolume.
Web: Symmetric MKI Negotiation <b>[IpProfile_EnableSymmetricMKI]</b>	For a description, see the global parameter EnableSymmetricMKI.
Web: MKI Size <b>[IpProfile_MKISize]</b>	For a description, see the global parameter SRTPTxPacketMKISize.
<b>Gateway Parameters</b>	
Web: Fax Signaling Method <b>[IpProfile_IsFaxUsed]</b>	For a description, see the global parameter IsFaxUsed.
Web: Play Ringback Tone to IP <b>[IpProfile_PlayRBTone2IP]</b>	For a description, see the global parameter PlayRBTone2IP.

Parameter	Description
Web: Enable Early Media <b>[IpProfile_EnableEarlyMedia]</b>	For a description, see the global parameter EnableEarlyMedia.
Web: Copy Destination Number to Redirect Number <b>[IpProfile_CopyDest2RedirectNumber]</b>	For a description, see the global parameter CopyDest2RedirectNumber.
Web: Media Security Behavior <b>[IpProfile_MediaSecurityBehaviour]</b>	For a description, see the global parameter MediaSecurityBehaviour.
Web: CNG Detector Mode <b>[IpProfile_CNGmode]</b>	For a description, see the global parameter CNGDetectorMode.
Web: Modems Transport Type <b>[IpProfile_VxxTransportType]</b>	For a description, see the global parameters V21ModemTransportType, V22ModemTransportType, V23ModemTransportType, V32ModemTransportType, and V34ModemTransportType.
Web: NSE Mode <b>[IpProfile_NSEMode]</b>	For a description, see the global parameter NSEMode.
Web: Number of Calls Limit <b>[IpProfile_CallLimit]</b>	<p>Defines the maximum number of concurrent calls (incoming and outgoing). If the number of concurrent calls reaches this limit, the device rejects any new incoming and outgoing calls belonging to this IP Profile.</p> <p>This parameter can also be set to the following:</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> = (Default) No limitation on calls.</li> <li>▪ <b>[0]</b> = Calls are rejected.</li> </ul> <p><b>Note:</b> For IP-to-IP calls, you can configure the device to route calls to an alternative IP Group when this maximum number of concurrent calls is reached. To do so, you need to add an alternative routing rule in the Outbound IP Routing table that reroutes the call to an alternative IP Group. You also need to add a rule to the Reason for Alternative Routing table to initiate an alternative rule for Tel-to-IP calls using cause 805.</p>
Web: Progress Indicator to IP <b>[IpProfile_ProgressIndicator2IP]</b>	For a description, see the global parameter ProgressIndicator2IP.
Web: Profile Preference <b>[IpProfile_IpPreference]</b>	<p>Defines the priority of the IP Profile, where "1" is the lowest and "20" the highest. If both IP and Tel Profiles apply to the same call, the coders and other common parameters of the preferred profile are applied to the call. If the preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.</p> <p><b>Note:</b> If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used. The order of the coders is determined by the preference.</p>
Web: Coder Group <b>[IpProfile_CodersGroupID]</b>	For a description, see the global parameter CodersGroup.
Web: Remote RTP Base UDP Port <b>[IpProfile_RemoteBaseUDPPort]</b>	For a description, see the global parameter RemoteBaseUDPPort.
Web: First Tx DTMF Option <b>[IpProfile_FirstTxDtmfOption]</b>	For a description, see the global parameter TxDTMFOption.

Parameter	Description
Web: Second Tx DTMF Option <b>[IpProfile_SecondTxDtmfOption]</b>	For a description, see the global parameter TxDTMFOption.
Web: Declare RFC 2833 in SDP <b>[IpProfile_RxDTMFOption]</b>	For a description, see the global parameter RxDTMFOption.
Web: Add IE In SETUP <b>[IpProfile_AddIEInSetup]</b>	For a description, see the global parameter AddIEInSetup.
Web: Enable QSIG Tunneling <b>[IpProfile_EnableQSIGTunneling]</b>	For a description, see the global parameter EnableQSIGTunneling.
Web: Enable Hold <b>[IpProfile_EnableHold]</b>	For a description, see the global parameter EnableHold.
<b>[IpProfile_EnableEarly183]</b>	For a description, see the global parameter EnableEarly183.
<b>[IpProfile_EarlyAnswerTimeout]</b>	For a description, see the global parameter EarlyAnswerTimeout.
<b>SBC Parameters</b>	
Web: Transcoding Mode <b>[IpProfile_TranscodingMode]</b>	For a description, see the global parameter TranscodingMode.
Web: Extension Coders Group ID <b>[IpProfile_SBCExtensionCodersGroupID]</b>	<p>Defines the Coder Group ID used for Extended (additional) coders added to the outgoing leg for this 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). Therefore, to allow IP entities to communicate with each other regardless of their capabilities, an Extended coders table with at least one coder that is supported by each IP entity needs to be assigned to each IP Group. Therefore, each offer destined to specific IP Groups includes this coder.</p> <p><b>Note:</b> To configure Coders Groups, see Configuring Coder Groups.</p>
Web: Allowed Coders Group ID <b>[IpProfile_SBCAllowedCodersGroupID]</b>	<p>Associates a Coders Group ID for defining the coders that can be used for this IP entity.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For a description of the Allowed Coders feature, see Restricting Coders.</li> <li>To configure Allowed Coders Groups, see Configuring Allowed Coder Groups on page 454.</li> </ul>
Web: Allowed Coders Mode <b>[IpProfile_SBCAllowedCodersMode]</b>	<p>Determines the mode of the Allowed Coders feature for this IP Profile.</p> <ul style="list-style-type: none"> <li><b>[0] Restriction</b> = In the incoming SDP offer, the device uses only coders that are also listed in the Allowed Coders Group; the rest are removed from the SDP offer (i.e., only coders common between SDP offered coders and Allowed Coders Group are used). If an Extension Coders Group is also selected (using the IP Profile's SBCExtensionCodersGroupID parameter), these coders are added to the SDP offer.</li> <li><b>[1] Preference</b> = The device re-arranges the priority (order)</li> </ul>

Parameter	Description
	<p>of the coders in the incoming SDP offer according to their order of appearance in the Allowed Coders Group list. This option also retains all the coders received in the SDP offer.</p> <ul style="list-style-type: none"> <li>▪ <b>[2] Restriction and Preference</b> = Performs both Restriction and Preference.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If the AllowedCodersGroup parameter is set to None, this parameter is not applicable.</li> <li>▪ To select the Allowed Coders Group ID, use the AllowedCodersGroup parameter.</li> <li>▪ To select the Extension Coders Group ID, use the CodersGroups parameter.</li> <li>▪ For more information on the Allowed Coders feature, see Restricting Coders.</li> </ul>
Web: SBC Preferences Mode <b>[SBCPreferencesMode]</b>	<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 (defined in the Allowed Coders Group table) in the outgoing SIP message (in the SDP).</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Doesn't Include Extensions</b> = (Default) Extension coders are added at the end of the coder list.</li> <li>▪ <b>[1] Include Extensions</b> = Extension coders and Allowed coders are arranged according to their order of appearance in the Allowed Coders Group table.</li> </ul> <p><b>Note:</b> If the SBCExtensionCodersGroupID parameter of the IP Profile table is set to None, this parameter is not applicable.</p>
Web: Diversion Mode <b>[IpProfile_SBCDiversionMode]</b>	<p>Determines the device's handling of the SIP Diversion header. For more information on interworking of the History-Info and Diversion headers, see Interworking SIP Diversion and History-Info Headers.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Don't Care</b> = (Default) Diversion header is not handled.</li> <li>▪ <b>[1] Add</b> = History-Info header converted to a Diversion header.</li> <li>▪ <b>[2] Remove</b> = Removes the Diversion header and the conversion to the History-Info header depends on the settings of the SBCHistoryInfoMode parameter.</li> </ul>
Web: History Info Mode <b>[IpProfile_SBCHistoryInfoMode]</b>	<p>Determines the device's handling of the History-Info header. For more information on interworking of the History-Info and Diversion headers, see Interworking SIP Diversion and History-Info Headers.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Don't Care</b> = (Default) History-Info header is not handled.</li> <li>▪ <b>[1] Add</b> = Diversion header converted to a History-Info header.</li> <li>▪ <b>[2] Remove</b> = History-Info header removed from the SIP dialog and the conversion to the Diversion header depends on the settings of the SBCDiversionMode parameter.</li> </ul>



Parameter	Description
Web: Media Security Behavior <b>[IpProfile_SBCMediaSecurityBehaviour]</b>	<p>Determines the transcoding method between SRTP and RTP and enforce an SBC leg to use SRTP or RTP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> As is = (Default) No special handling for RTP\SRTP is done.</li> <li><b>[1]</b> SRTP = SBC legs negotiate only SRTP media lines, and RTP media lines are removed from the incoming SDP offer\answer.</li> <li><b>[2]</b> RTP = SBC legs negotiate only RTP media lines, and SRTP media lines are removed from the incoming offer\answer.</li> <li><b>[3]</b> Both = Each offer\answer is extended (if not already) to two media lines - one RTP and the other SRTP.</li> </ul> <p>If two SBC legs (after offer\answer negotiation) use different security types (i.e., one RTP and the other SRTP), the device performs RTP-SRTP transcoding. To transcode between RTP and SRTP, the following prerequisites must be met:</p> <ul style="list-style-type: none"> <li>At least one supported SDP "crypto" attribute and parameters</li> <li>EnableMediaSecurity must be set to 1</li> </ul> <p>If one of the above transcoding prerequisites is not met, then:</p> <ul style="list-style-type: none"> <li>any value other than "As is" is discarded.</li> <li>if the incoming offer is SRTP, force transcoding, coder transcoding, and DTMF extensions are not applied.</li> </ul>
Web: RFC 2833 Behavior <b>[IpProfile_SBCRFC2833Behavior]</b>	<p>Determines the RFC 2833 SDP offer\answer negotiation.</p> <ul style="list-style-type: none"> <li><b>[0]</b> As is = (Default) The device does not intervene in the RFC 2833 negotiation.</li> <li><b>[1]</b> 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).</li> <li><b>[2]</b> Disallow = The device removes RFC 2833 from the incoming offer.</li> </ul>
Web: Alternative DTMF Method <b>[IpProfile_SBCAlternativeDTMFMethod]</b>	<p>The device's first priority for DTMF method at each leg is RFC 2833. Therefore, if a specific leg negotiates RFC 2833 successfully, the chosen DTMF method for this leg is RFC 2833. For legs where RFC 2833 is not negotiated successfully, the device uses this parameter to determine the chosen DTMF method for the leg.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Don't care = (Default) The device does not attempt to interwork any special DTMF method.</li> <li><b>[1]</b> Transparent = In Band</li> <li><b>[2]</b> INFO - Cisco</li> <li><b>[3]</b> INFO - Nortel</li> <li><b>[4]</b> INFO - Lucent = INFO, Korea</li> </ul>
Web: P-Asserted-Identity <b>[IpProfile_SBCAssertIdentity]</b>	For a description, see the global parameter SBCAssertIdentity.
Web: SBC Fax Coders Group ID <b>[IpProfile_SBCFaxCodersGroupID]</b>	Selects the supported fax coders (Coders Group ID) for fax negotiation. Coders Groups are configured in the Coders Group Settings table.

Parameter	Description
Web: SBC Fax Behavior <b>[IpProfile_SBCFaxBehavior]</b>	<p>Defines the negotiation method for fax offer.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Pass fax transparently, without interference.</li> <li>▪ <b>[1]</b> = Handle fax according to fax settings in the IP Profile for all offer-answer transactions (including the initial INVITE).</li> <li>▪ <b>[2]</b> = Handle fax according to fax settings in the IP Profile for all re-INVITE offer-answer transactions (except for initial INVITE).</li> </ul>
Web: SBC Fax Offer Mode <b>[IpProfile_SBCFaxOfferMode]</b>	<p>Defines the coders included in the outgoing SDP offer (sent to the called "fax").</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> All = (Default) Use only (and all) the coders of the selected Coders Group ID configured using the SBCFaxCodersGroupID parameter.</li> <li>▪ <b>[1]</b> Single = Use only one coder. If a coder in the incoming offer (from the calling "fax") matches a coder in the SBCFaxCodersGroupID, then the device uses this coder. If no match exists, then the device uses the first coder listed in the Coders Group ID (SBCFaxCodersGroupID).</li> </ul>
Web: SBC Fax Answer Mode <b>[IpProfile_SBCFaxAnswerMode]</b>	<p>Defines the coders included in the outgoing SDP answer (sent to the calling "fax").</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Use matched coders between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group ID (configured using the SBCFaxCodersGroupID parameter).</li> <li>▪ <b>[1]</b> = (Default) Use only one coder. If the incoming answer (from the called "fax") includes a coder that matches a coder match between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group ID (SBCFaxCodersGroupID, then the device uses this coder. If no match exists, the device uses the first listed coder of the matched coders between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group ID.</li> </ul>
Web: SBC Session Expires Mode <b>[IpProfile_SBCSessionExpiresMode]</b>	<p>Determines the required session expires mode of the IP entity.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Transparent = (Default) The device does not interfere with the session expires negotiation.</li> <li>▪ <b>[1]</b> Observer = If the SIP Session-Expires header is present, the device does not interfere, but maintains an independent timer for each leg to monitor the session. If the session is not refreshed on time, the device disconnects the call.</li> <li>▪ <b>[2]</b> Not Supported = The device does not allow a session timer with this IP entity.</li> <li>▪ <b>[3]</b> Supported = The device enables the session timer with this IP entity. If the incoming SIP message does not include any session timers, the device adds the session timer information to the sent message. You can configure the value of the Session-Expires and Min-SE headers, using the SBCSessionExpires and SBCMinSE parameters, respectively.</li> </ul>

Parameter	Description
Web: SBC Remote Early Media RTP <b>[IpProfile_SBCRemoteEarlyMediaRTP]</b>	<p>Defines whether the destination UA sends RTP immediately after it sends 18x response.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Immediate = (Default) Remote client sends RTP immediately after it sends 18x response with early media. Device forwards 18x and RTP as is.</li> <li><b>[1]</b> Delayed = After sending 18x response, the remote client waits before sending RTP (e.g., Microsoft Lync environment). For the device's handling of this remote UA support, see Interworking SIP Early Media.</li> </ul>
Web: SBC Remote Can Play Ringback <b>[IpProfile_SBCRemoteCanPlayRingback]</b>	<p>Defines whether the destination UA can play a local ringback tone.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = UA does not support local ringback tone. The device sends 18x with delayed SDP to the UA.</li> <li><b>[1]</b> Yes = (Default) UA supports local ringback tone. For the device's handling of this remote UA support, see Interworking SIP Early Media.</li> </ul>
Web: SBC Remote Supports RFC 3960 <b>[IpProfile_SBCRemoteSupportsRFC3960]</b>	<p>Defines whether the destination UA is capable of receiving 18x messages with delayed RTP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = (Default) UA does not support receipt of 18x messages with delayed RTP. For the device's handling of this remote UA support, see Interworking SIP Early Media.</li> <li><b>[1]</b> Supported = UA is capable of receiving 18x messages with delayed RTP.</li> </ul>
Web: SBC Multiple 18x Support <b>[IpProfile_SBCRemoteMultiple18xSupport]</b>	<p>Determines whether multiple 18x responses (including 180 Ringing, 181 Call is Being Forwarded, 182 Call Queued, and 183 Session Progress) are forwarded to the caller.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = Only the first 18x response is forwarded to the caller.</li> <li><b>[1]</b> Supported = (Default) Multiple 18x responses are forwarded to the caller.</li> </ul>
Web: SBC Early Media Response Type <b>[IpProfile_SBCRemoteEarlyMediaResponseType]</b>	<p>Determines the SIP provisional response type - 180 or 183 - for forwarding early media to the caller.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Transparent = (Default) All early media response types are supported; the device forwards all responses as is (unchanged).</li> <li><b>[1]</b> 180 = Early media is sent as 180 response only.</li> <li><b>[2]</b> 183 = Early media is sent as 183 response only.</li> </ul>
Web: SBC Remote Update Support <b>[IpProfile_SBCRemoteUpdateSupport]</b>	<p>Determines whether endpoints support the UPDATE method.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = UPDATE method is not supported.</li> <li><b>[1]</b> Supported Only After Connect = UPDATE method is supported only after the call is connected.</li> <li><b>[2]</b> Supported = (Default) UPDATE method is supported during call setup and after call establishment.</li> </ul>

Parameter	Description
Web: SBC Remote Re-Invite Support <b>[IpProfile_SBCRemoteReinviteSupport]</b>	<p>Determines whether the destination UA of the re-INVITE request supports re-INVITE messages and if so, whether it supports re-INVITE with or without SDP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = re-INVITE is not supported and the device does not forward re-INVITE requests. The device sends a SIP response to the re-INVITE request, which can either be a success or a failure, depending on whether the device can bridge the media between the endpoints.</li> <li><b>[1]</b> Supported with SDP = re-INVITE is supported, but only with SDP. If the incoming re-INVITE arrives without SDP, the device creates an SDP and adds it to the outgoing re-INVITE.</li> <li><b>[2]</b> Supported = (Default) re-INVITE is supported with or without SDP.</li> </ul>
Web: SBC Remote Refer Behavior <b>[IpProfile_SBCRemoteReferBehavior]</b>	For a description, see the global parameter SBCReferBehavior.
Web: SBC Remote Early Media Support <b>[IpProfile_SBCRemoteEarlyMediaSupport]</b>	<p>Determines whether a remote side can accept early media or not.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = Early media is not supported.</li> <li><b>[1]</b> Supported = (Default) Early media is supported.</li> </ul>
Web: SBC Remote 3xx Behavior <b>[IpProfile_SBCRemote3xxBehavior]</b>	For a description, see the global parameter SBC3xxBehavior.
Web: SBC Remote Delayed Offer Support <b>[IpProfile_SBCRemoteDelayedOfferSupport]</b>	<p>Determines whether the remote endpoint supports delayed offer (i.e., initial INVITEs without an SDP offer).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = Initial INVITE requests without SDP are not supported.</li> <li><b>[1]</b> Supported = (Default) Initial INVITE requests without SDP are supported.</li> </ul> <p>Note: For this parameter to function properly, a valid Extension Coders Group ID needs to be configured for IP Profiles that do not support delayed offer.</p>
Web: SBC PRACK Mode <b>[IpProfile_SbcPrackMode]</b>	<p>Determines the PRACK mode required at the remote side:</p> <ul style="list-style-type: none"> <li><b>[1]</b> Optional = PRACK is optional for these UAs. If required, the device performs the PRACK process on behalf of the destination UA.</li> <li><b>[2]</b> Mandatory = PRACK is required for these UAs. Calls from UAs that do not support PRACK are rejected. Calls destined to these UAs are also required to support PRACK.</li> <li><b>[3]</b> Transparent (default) = The device does not intervene with the PRACK process and forwards the request as is.</li> </ul>
Web: SBC Enforce MKI Size <b>[IpProfile_SBCEnforceMKISize]</b>	<p>Enables MKI length negotiation for SRTP-to-SRTP flows between SIP networks (i.e., IP Groups). This feature includes the capability of modifying the MKI length on the inbound or outbound SBC call leg, using IP Profiles.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Device forwards the MKI size as is.</li> <li><b>[1]</b> Enable = Device changes the MKI length according to the settings of the IP Profile parameter, MKISize.</li> </ul>

Parameter	Description
Web: SBC RFC2833 DTMF Payload Type Value <b>[IpProfile_SBC2833DTMFPayloadType]</b>	<p>Defines the RFC 2833 DTMF Payload Type for a specific SBC leg. This enables the interworking of the DTMF payload type for RFC 2833 between different SBC call legs. For example, if two entities require different DTMF payload types, the SDP offer received by the device from one entity is forwarded to the destination entity with its payload type replaced with the configured payload type, and vice versa.</p> <p>The value range is 96 to 127. The default is 0 (i.e., the device forwards the received payload type as is).</p>
Web: SBC User Registration Time <b>[IpProfile_SBCUserRegistrationTime]</b>	For a description, see the global parameter SBCUserRegistrationTime.
Web: SBC Remote Hold Format <b>[IPProfile_SBCRemoteHoldFormat]</b>	<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"> <li>▪ <b>[0]</b> transparent = Device forwards SDP as is.</li> <li>▪ <b>[1]</b> send-only = Device sends SDP with 'a=sendonly'.</li> <li>▪ <b>[2]</b> send only 0.0.0.0 = Device sends SDP with 'a=sendonly' and 'c=0.0.0.0'.</li> <li>▪ <b>[3]</b> inactive = Device sends SDP with 'a=inactive'.</li> <li>▪ <b>[4]</b> inactive 0.0.0.0 = Device sends SDP with 'a=inactive' and 'c=0.0.0.0'.</li> <li>▪ <b>[5]</b> not supported = Used when remote side cannot identify a call-hold message. The device terminates the received call-hold message (re-INVITE / UPDATE) and sends a 200 OK to the initiator of the call hold. The device plays a held tone to the held party if the 'SBC Play Held Tone' parameter is set to Yes.</li> </ul>
Web: SBC Play Held Tone <b>[IpProfile_SBCPlayHeldTone]</b>	<p>Enables the device to play a held tone to the held party. This is useful if the held party does not support playing a local held tone, or for IP entities initiating call hold that do not support the generation of held tones.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No (default)</li> <li>▪ <b>[1]</b> Yes</li> </ul> <p><b>Note:</b> If this parameter is set to Yes, the device plays the tone only if the 'SBC Remote Hold Format' parameter is set to transparent, send-only, send only 0.0.0.0, or not supported.</p>
Web: SBC Reliable Held Tone Source <b>[IPProfile_ReliableHoldToneSource]</b>	<p>Enables the device to consider the received call-hold request (re-INVITE/UPDATE) with SDP containing 'a=sendonly', as genuine.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No (default) = Even if the received SDP contains 'a=sendonly', the device plays a held tone to the held party. This is useful in cases where the initiator of the call hold does not support the generation of held tones.</li> <li>▪ <b>[1]</b> Yes = If the received SDP contains 'a=sendonly', the device does not play a held tone to the held party (and assumes that the initiator of the call hold plays the held tone).</li> </ul> <p><b>Note:</b> The device plays a held tone only if the 'SBC Play Held Tone' parameter is set to Yes.</p>

## Reader's Notes

# Part V

## Gateway and IP-to-IP Application





## 24 IP-to-IP Routing Overview

This section describes configuration of the Gateway and IP-to-IP applications. The Gateway application refers to IP-to-Tel (PSTN) call routing and vice versa. The IP-to-IP application refers to call routing of calls received from the IP and forwarded to an IP destination. For a description of the IP-to-IP application, see IP-to-IP Routing Application on page 253.



### Notes:

- In some areas of the Web interface, the term "GW" and "IP2IP" application refers to the Gateway and IP-to-IP applications, respectively.
- The terms *IP-to-Tel* and *Tel-to-IP* refer to the direction of the call relative to the device. IP-to-Tel refers to calls received from the IP network and destined to the PSTN/PBX (i.e., telephone connected directly or indirectly to the device); Tel-to-IP refers to calls received from telephones connected directly to the device's FXS ports or from the PSTN/PBX, and destined for the IP network.
- FXO (Foreign Exchange Office) is the interface replacing the analog telephone and connects to a Public Switched Telephone Network (PSTN) line from the Central Office (CO) or to a Private Branch Exchange (PBX). The FXO is designed to receive line voltage and ringing current, supplied from the CO or the PBX (just like an analog telephone). An FXO VoIP device interfaces between the CO/PBX line and the Internet.
- FXS (Foreign Exchange Station) is the interface replacing the Exchange (i.e., the CO or the PBX) and connects to analog telephones, dial-up modems, and fax machines. The FXS is designed to supply line voltage and ringing current to these telephone devices. An FXS VoIP device interfaces between the analog telephone devices and the Internet.

The device's IP-to-IP application supports IP-to-IP VoIP call routing (or SIP Trunking). The IP-to-IP call routing application enables enterprises to seamlessly connect their IP-based PBX (IP-PBX) to SIP trunks, typically provided by Internet Telephony Service Providers (ITSP). The device enables the enterprise to communicate with the PSTN network (local and overseas) through the ITSP, which interfaces directly with the PSTN. Therefore, the IP-to-IP application enables enterprises to replace the bundles of physical PSTN wires with SIP trunks provided by ITSPs and use VoIP to communicate within and outside the enterprise network using its standard Internet connection. At the same time, the device can also provide an interface with the traditional PSTN network, enabling PSTN fallback in case of IP connection failure with the ITSPs.

The device also supports multiple SIP Trunking. This can be useful in scenarios where if a connection to one ITSP fails, the call can immediately be transferred to another ITSP. In addition, by allowing multiple SIP trunks where each trunk is designated a specific ITSP, the device can route calls to an ITSP based on call destination (e.g., country code).

In addition to providing VoIP communication within the enterprise's LAN, the device enables the enterprise to communicate outside of the corporate LAN using SIP Trunking. This includes remote (roaming) IP-PBX users, for example, employees using their laptops to communicate with one another from anywhere in the world such as at airports.

The IP-to-IP application can be implemented by enterprises in the following example scenarios:

- VoIP between an enterprise's headquarters and remote branch offices
- VoIP between an enterprise and the PSTN through an ITSP

The IP-to-IP call routing capability is feature-rich, allowing interoperability with different ITSPs:

- Easy and smooth integration with multiple ITSP SIP trunks.
- Supports SIP registration and authentication with ITSP servers (on behalf of the enterprise's IP telephony system) even if the enterprise's IP telephony system does not support registration and authentication.
- Supports SIP-over-UDP, SIP-over-TCP, and SIP-over-TLS transport protocols, one of which is generally required by the ITSP.
- Provides alternative routing to different destinations (to another ITSP or the PSTN) when the connection with an ITSP network is down.
- Provides fallback to the legacy PSTN telephone network upon Internet connection failure.
- Provides Transcoding from G.711 to G.729 coder with the ITSP for bandwidth reduction.
- Supports SRTP, providing voice traffic security toward the ITSP.
- IP-to-IP routing can be used in combination with the regular Gateway application. For example, an incoming IP call can be sent to an E1/T1 span or it can be forwarded to an IP destination.

Therefore, the device provides the ideal interface between the enterprise IP-PBX and the ITSP SIP trunk.

The device's IP-to-IP application handles and terminates SIP methods and responses at each leg independently:

- Initiating-dialog INVITE: terminated at one leg and initiated on the other leg, 180\182\183\200\4xx uses the same logic and same limitations, in some cases the result may be a different response code.
- OPTIONS: terminated at each leg independently.
- INFO: only specific INFO's (such as DTMF) are handled; other types are omitted.
- UPDATE: terminated at each leg independently and may cause only changes in the RTP flow - Hold\Retrieve are the only exceptions that traverse the two legs.
- Re-INVITE: terminated at each leg independently and may cause only changes in the RTP flow - Hold\Retrieve are the only exceptions that traverse the two legs.
- PRACK: terminated at each leg independently.
- REFER (within a dialog): terminated at each leg independently.
- 3xx Responses: terminated at each leg independently.
- 401\407 responses to initial INVITE: in case the back-to-back session is associated with an Account, the responses is terminated at the receiving leg; in other cases, the responses are passed transparently.
- REGISTER: handled only in cases associated with a User-type IP Group - Contact, To, From specific parameters are omitted.

## 24.1 Theory of Operation

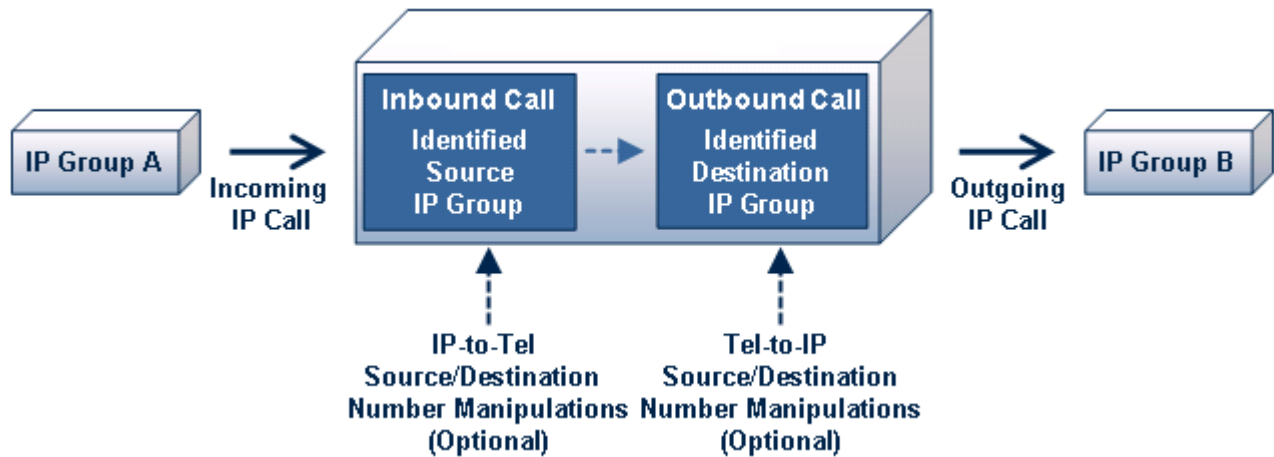
The device's IP-to-IP SIP session is performed by implementing Back-to-Back User Agent (B2BUA). The device acts as a user agent for both ends (*legs*) of the SIP call (from call establishment to termination). The session negotiation is performed independently for each call leg, using global parameters such as coders or using IP Profiles associated with each call leg to assign different configuration behaviors for these two IP-to-IP call legs.

For the maximum number of supported IP-to-IP sessions, see DSP Templates on page 897.

The device also supports NAT traversal for SIP clients behind NAT, where the device is defined with a global IP address.

The figure below provides a simplified illustration of the device's handling of IP-to-IP call routing:

**Figure 24-1: Basic Schema of the Device's IP-to-IP Call Handling**



The basic IP-to-IP call handling process can be summarized as follows:

1. Incoming IP calls are identified as belonging to a specific logical entity in the network referred to as a *Source IP Group*, according to Inbound IP Routing rules.
2. The Source IP Group is sent to a specific IP Group referred to as a *Destination IP Group*; the IP destination address being as configured by the *Proxy Set* associated with the Destination IP Group.
3. Number manipulation can be done on inbound and outbound legs.

The following subsections discuss the main terms associated with the IP-to-IP call routing application.

### 24.1.1 Proxy Sets

A Proxy Set is a group of Proxy servers (for Proxy load balancing and redundancy) defined by IP address or fully qualified domain name (FQDN). The Proxy Set is assigned to Server-type IP Groups only, representing the address of the IP Group to where the device sends the INVITE message (i.e., the **destination** of the call). Typically, for IP-to-IP call routing, two Proxy Sets are defined for call destination – one for each leg (i.e., one for each IP Group) of the call (i.e., both directions).

### 24.1.2 IP Groups

An IP Group represents a logical SIP entity in the device's network environment such as an ITSP SIP trunk, Proxy/Registrar server, IP-PBX, or remote IP-PBX users. The address of the IP Group is typically defined by its associated Proxy Set.

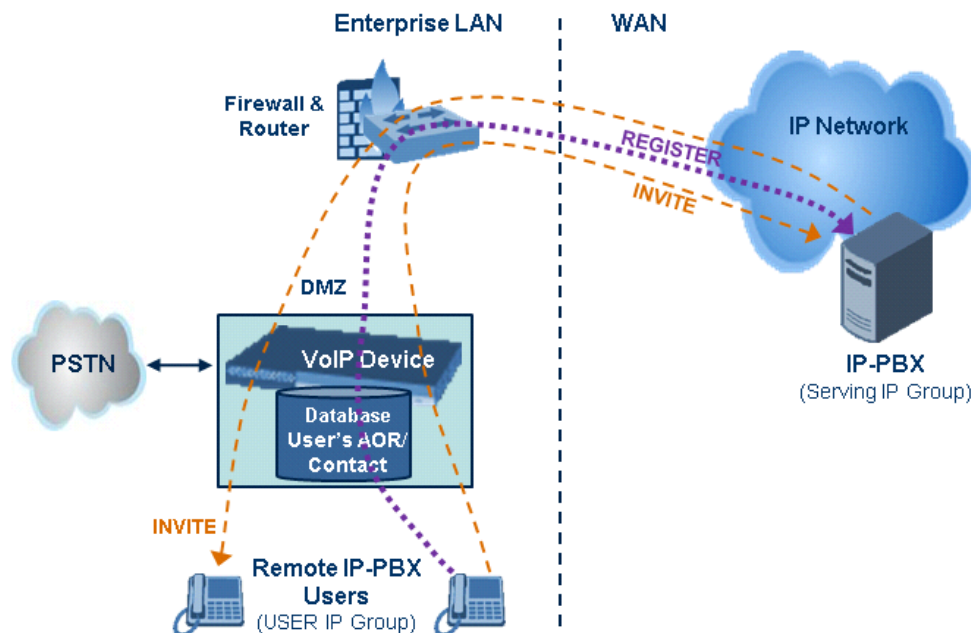
The opposite legs of the call are each presented by an IP Group; one being a *Serving* IP Group the other a *Served* IP Group. The Serving IP Group denotes the IP Group that provides service (e.g., ITSP) to the Served IP Group (e.g., IP-PBX). This is the IP Group to where the device sends INVITE messages received from the Served IP Group as well as REGISTER messages for registering on behalf of the Served IP Group.

IP Group can be a *Server* or *User* type. For Server-type IP Groups (e.g., ITSP or IP-PBX), the destination address (defined by the Proxy Set) is known. In contrast, User-type IP Groups represents groups of users whose location is dynamically obtained by the device when REGISTER requests and responses traverse (or are terminated) by the device. Generally, these are remote IP-PBX users (e.g., IP phones and soft phones).

For registrations of User-type IP Groups, the device updates its internal database with the AOR and Contacts of the users (see the figure below) Digest authentication using SIP

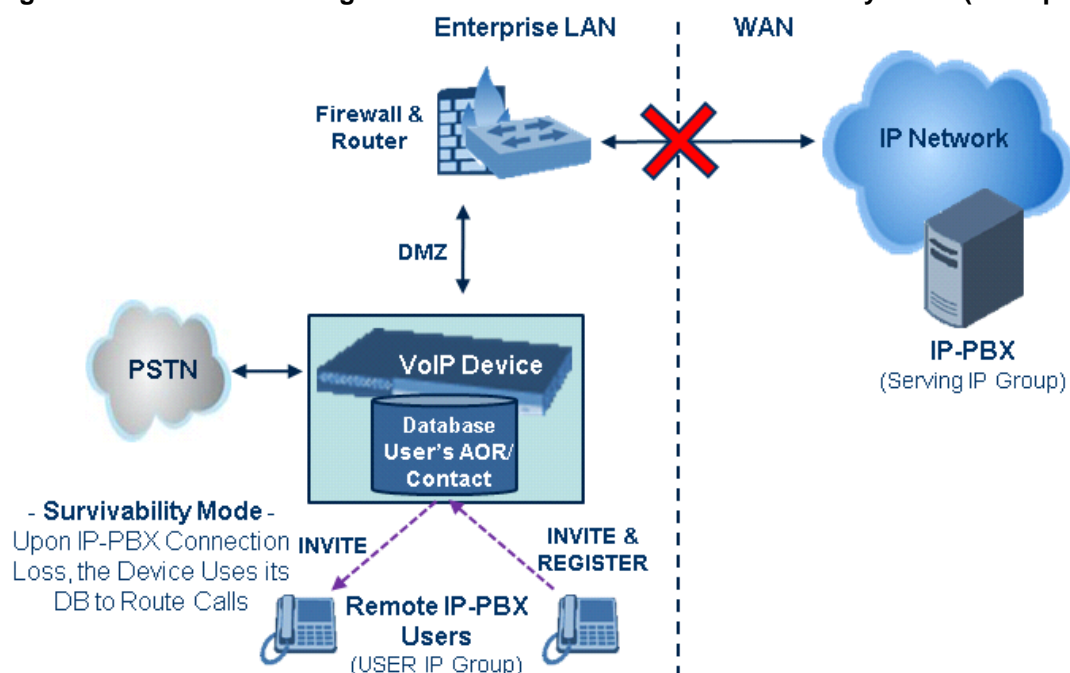
401/407 responses, if needed, is done by the Serving IP Group (e.g., IP-PBX). The device forwards these responses directly to the remote SIP users. For a call to a registered remote user, the device searches its dynamic database using the Request URI for an entry that matches a registered AOR or Contact. Once an entry is found, the IP destination is obtained and a SIP request is then sent to the user.

**Figure 24-2: IP-to-IP Routing/Registration/Authentication of Remote IP-PBX Users (Example)**



The device also supports the IP-to-IP call routing Survivability mode feature (see the figure below) for User-type IP Groups. The device stores in its database REGISTER messages sent by the clients of the User-type IP Group. If communication with the Serving IP Group (e.g., IP-PBX) fails, the User-type IP Group enters into Survivability mode in which the device uses its database for routing calls between the clients of the User-type IP Group. The RTP packets between the clients traverse through the device. When the Serving IP Group is available again, the device returns to normal mode, sending INVITE and REGISTER messages to the Serving IP Group.

**Figure 24-3: IP-to-IP Routing for IP-PBX Remote Users in Survivability Mode (Example)**



### 24.1.3 Inbound and Outbound IP Routing Rules

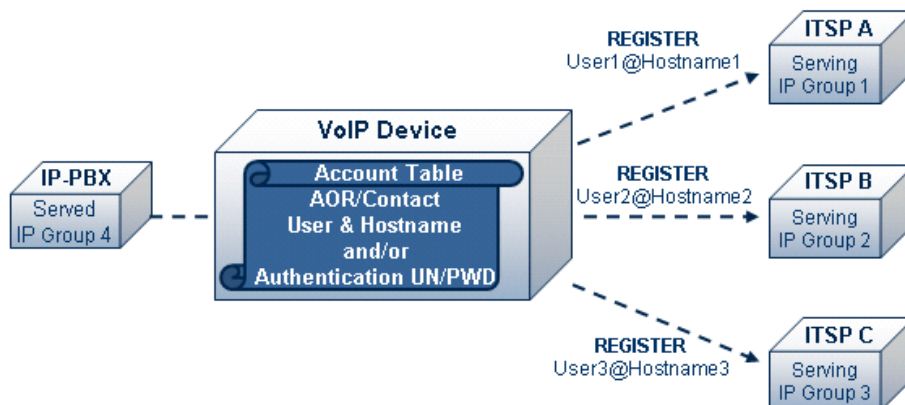
The device's IP-to-IP call routing is performed using the following two routing rule stages:

1. **Inbound IP Routing Mapping Rule:** Identifies the received call as an IP-to-IP call based on various characteristics such as the call's source IP address, and assigns it to an IP Group.
2. **Outbound IP Routing Mapping Rule:** Determines the destination (i.e., IP address) to where the incoming call associated with a specific source IP Group is finally routed. The destination address is typically denoted by another IP Group (destination IP Group) and therefore, the call is sent to the IP address that is defined by the Proxy Set associated with this IP Group. If the destination is a User-type IP Group, the device searches for a match between the request-URI of the received INVITE to an AOR registration record in the device's database. If a match is found, the INVITE is sent to the IP address of the registered contact.

### 24.1.4 Accounts

Accounts are used by the device to register to a Serving IP Group (e.g., an ITSP) on behalf of a Served IP Group (e.g., IP-PBX). This is necessary for ITSPs that require registration to provide services. Accounts are also used for defining user name and password for digest authentication (with or without registration) if required by the ITSP. Multiple Accounts per Served IP Group can be configured for registration to more than one Serving IP Group (e.g., an IP-PBX that requires registering to multiple ITSP's).

**Figure 24-4: Registration with Multiple ITSP's on Behalf of IP-PBX**



## 24.2 IP-to-IP Routing Configuration Example

This section provides step-by-step procedures for configuring IP-to-IP call routing. These procedures are based on the setup example described below. In this example, the device serves as the communication interface between the enterprise's IP-PBX (located on the LAN) and the following network entities:

- ITSP SIP trunks (located on the WAN)
- Remote IP-PBX users (located on the WAN)
- Local PSTN network

Calls from the Enterprise are routed according to destination.

This example assumes the following:

- The device has the public IP address 212.25.125.136 and is connected to the enterprise's firewall/NAT demilitarized zone (DMZ) network, providing the interface

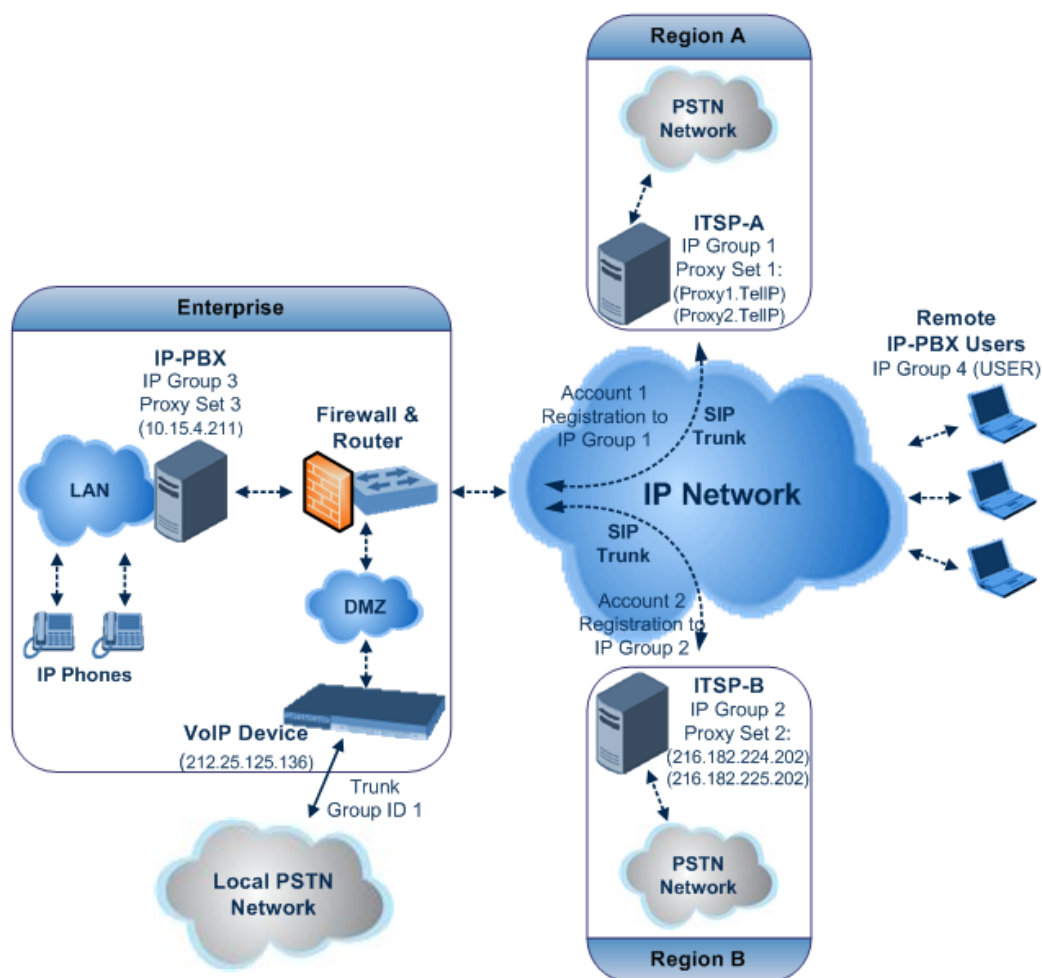
between the IP-PBX, and two ITSP's and the local PSTN.

- The enterprise has an IP-PBX located behind a Firewall/NAT:
  - IP-PBX IP address: 10.15.4.211
  - Transport protocol: UDP
  - Voice coder: G.711
  - IP-PBX users: 4-digit length extension number and served by two ITSPs.
  - The enterprise also includes remote IP-PBX users that communicate with the IP-PBX via the device. All dialed calls from the IP-PBX consisting of four digits starting with digit "4" are routed to the remote IP-PBX users.
- Using SIP trunks, the IP-PBX connects (via the device) to two different ITSP's:
  - **ITSP-A:**
    - ◆ Implements Proxy servers with fully qualified domain names (FQDN): "Proxy1.ITSP-A" and "Proxy2.ITSP-B", using TLS.
    - ◆ Allocates a range of PSTN numbers beginning with +1919, which is assigned to a range of IP-PBX users.
    - ◆ Voice coder: G.723.
  - **ITSP-B:**
    - ◆ Implements Proxy servers with IP addresses 216.182.224.202 and 216.182.225.202, using TCP.
    - ◆ Allocates a range of PSTN numbers beginning with 0200, which is assigned to a range of IP-PBX users.
    - ◆ Voice coder: G.723.
- Registration and authentication is required by both ITSP's, which is performed by the device on behalf of the IP-PBX. The SIP REGISTER messages use different URI's (host name and contact user) in the From, To, and Contact headers per ITSP as well as username and password authentication.
- Outgoing calls from IP-PBX users are routed according to destination:
  - If the calls are dialed with the prefix "+81", they are routed to ITSP-A (Region A).
  - If the calls are dialed with the prefix "9", they are routed to the local PSTN network.
  - For all other destinations, the calls are routed to ITSP-B.
- The device is also connected to the PSTN through a traditional T1 ISDN trunk for local incoming and outgoing calls. Calls dialed from the enterprise's IP-PBX with prefix '9' are sent to the local PSTN. In addition, in case of Internet interruption and loss of connection with the ITSP trunks, all calls are rerouted to the PSTN.

The figure below provides an illustration of this example scenario:



Figure 24-5: SIP Trunking Setup Scenario Example



The steps for configuring the device according to the scenario above can be summarized as follows:

- Enable the IP-to-IP feature (see 'Step 1: Enable the IP-to-IP Capabilities' on page 260).
- Configure the number of media channels (see 'Step 2: Configure the Number of Media Channels' on page 260).
- Configure a Trunk Group for interfacing with the local PSTN (see 'Step 3: Define a Trunk Group for the Local PSTN' on page 260).
- Configure Proxy Sets (see 'Step 4: Configure the Proxy Sets' on page 261).
- Configure IP Groups (see 'Step 5: Configure the IP Groups' on page 263).
- Configure Registration Accounts (see 'Step 6: Configure the Account Table' on page 264).
- Configure IP Profiles (see 'Step 7: Configure IP Profiles for Voice Coders' on page 265).
- Configure inbound IP routing rules (see 'Step 8: Configure Inbound IP Routing' on page 266).
- Configure outbound IP routing rules (see 'Step 9: Configure Outbound IP Routing' on page 268).
- Configure destination phone number manipulation (see 'Step 10: Configure Destination Phone Number Manipulation' on page 269).

## 24.2.1 Step 1: Enable the IP-to-IP Capabilities

This step describes how to enable the device's IP-to-IP application.

➤ **To enable IP-to-IP capabilities:**

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** submenu > **Applications Enabling**).
2. From the 'IP to IP Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Save the setting to flash memory ("burn") with a device reset.



**Note:** For the IP-to-IP Application feature, the device must also be installed with the appropriate Software License Key.

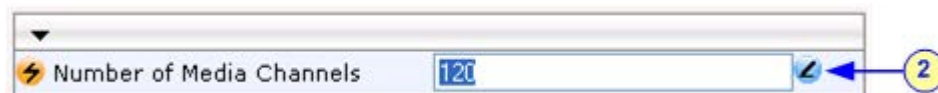
## 24.2.2 Step 2: Configure the Number of Media Channels

The number of media channels represents the number of digital signaling processors (DSP) channels that the device allocates to IP-to-IP calls. The remaining DSP channels can be used for PSTN calls. Two IP media channels are used per IP-to-IP call.

➤ **To configure the number of media channels:**

1. Open the IP Media Settings page (**Configuration** tab > **VoIP** menu > **IP Media** > **IP Media Settings**).

**Figure 24-6: Defining Required Media Channels**



2. In the 'Number of Media Channels' field, enter the required number of media channels (in the example above, "120" to enable up to 60 IP-to-IP calls).
3. Click **Submit**.
4. Save the settings to flash memory ("burn") with a device reset (see 'Saving Configuration' on page 532).

## 24.2.3 Step 3: Define a Trunk Group for the Local PSTN

For incoming and outgoing local PSTN calls with the IP-PBX, you need to define the Trunk Group ID (#1) for the T1 ISDN trunk connecting the device to the local PSTN. This Trunk Group is also used for alternative routing to the PSTN if connectivity with the ITSP fails.

➤ **To configure the Trunk Group for local PSTN:**

1. Open the Trunk Group Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Trunk Group** > **Trunk Group**).
2. Configure Trunk Group ID #1 (as shown in the figure below):
  - From the 'From Trunk' and 'To Trunk' drop-down lists, select **1** to indicate Trunk 1 for this Trunk Group.
  - In the 'Channels' field, enter the Trunk channels or ports assigned to the Trunk Group (e.g. 1-31 for E1 and 1-24 for T1).



- In the 'Phone Number' field, enter any phone number (logical) for this Trunk (e.g. 1000).
- In the 'Trunk Group ID' field, enter "1" as the ID for this Trunk Group.

Add Phone Context As Prefix		Disable	
Trunk Group Index		1-12	

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 PRI	1	1	1-31	1000	1	
2							

3. Configure the Trunk in the Trunk Settings page (**Configuration** tab > **VoIP** menu > **PSTN > Trunk Settings**).

## 24.2.4 Step 4: Configure the Proxy Sets

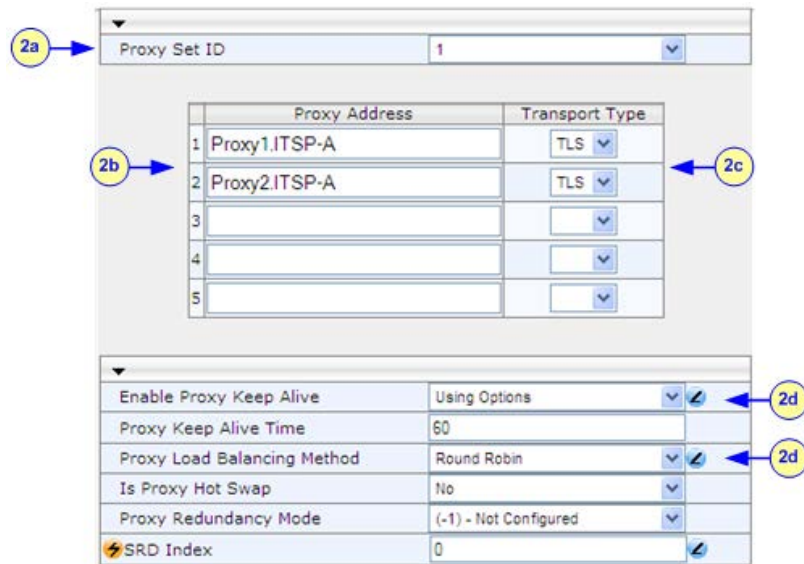
The Proxy Sets represent the actual destination (IP address or FQDN) to which the call is routed. These Proxy Sets are later assigned to IP Groups (see 'Step 5: Configure the IP Groups' on page 263).

This step describes how to configure the following Proxy Sets:

- Proxy Set ID #1 with two FQDN's for ITSP-A
- Proxy Set ID #2 with two IP addresses for ITSP-B
- Proxy Set ID #3 with an IP address for the IP-PBX

### ➤ To configure the Proxy Sets:

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network > Proxy Sets Table**).
2. Configure Proxy Set ID #1 for ITSP-A:
  - a. From the 'Proxy Set ID' drop-down list, select **1**.
  - b. In the 'Proxy Address' column, enter the FQDN of ITSP-A SIP trunk Proxy servers (e.g., "Proxy1.ITSP-A" and "Proxy2. ITSP-A").
  - c. From the 'Transport Type' drop-down list corresponding to the Proxy addresses entered above, select **TLS**.
  - d. In the 'Enable Proxy Keep Alive' drop-down list, select **Using Options**, and then in the 'Proxy Load Balancing Method' drop-down list, select **Round Robin**.

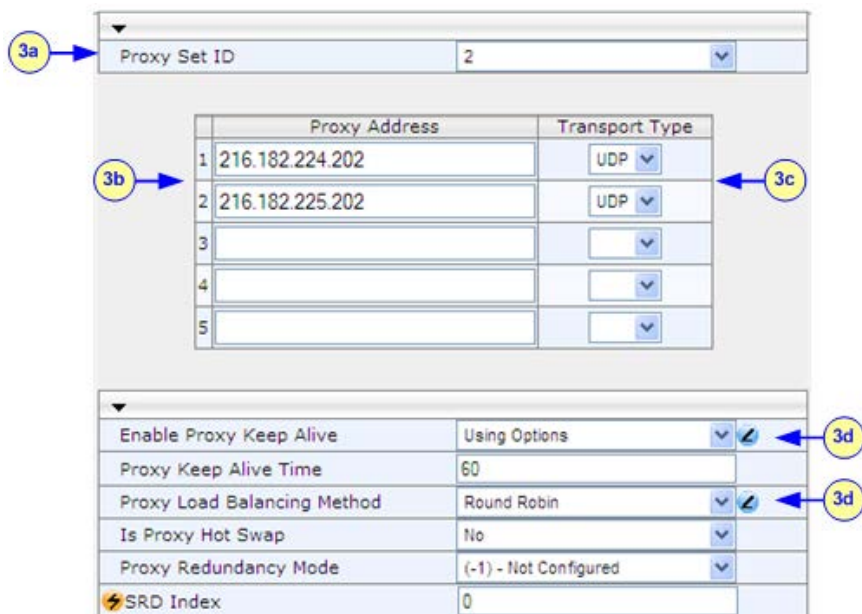
**Figure 24-7: Proxy Set ID #1 for ITSP-A**


Proxy Set ID: 1

	Proxy Address	Transport Type
1	Proxy1.ITSP-A	TLS
2	Proxy2.ITSP-A	TLS
3		
4		
5		

Enable Proxy Keep Alive: Using Options  
 Proxy Keep Alive Time: 60  
 Proxy Load Balancing Method: Round Robin  
 Is Proxy Hot Swap: No  
 Proxy Redundancy Mode: (-1) - Not Configured  
 SRD Index: 0

3. Configure Proxy Set ID #2 for ITSP-B:
  - a. From the 'Proxy Set ID' drop-down list, select **2**.
  - b. In the 'Proxy Address' column, enter the IP addresses of the ITSP-B SIP trunk (e.g., "216.182.224.202" and "216.182.225.202").
  - c. From the 'Transport Type' drop-down list corresponding to the IP address entered above, select **UDP**.
  - d. In the 'Enable Proxy Keep Alive' drop-down list, select "Using Options", and then in the 'Proxy Load Balancing Method' drop-down list, select **Round Robin**.

**Figure 24-8: Proxy Set ID #2 for ITSP-B**


Proxy Set ID: 2

	Proxy Address	Transport Type
1	216.182.224.202	UDP
2	216.182.225.202	UDP
3		
4		
5		

Enable Proxy Keep Alive: Using Options  
 Proxy Keep Alive Time: 60  
 Proxy Load Balancing Method: Round Robin  
 Is Proxy Hot Swap: No  
 Proxy Redundancy Mode: (-1) - Not Configured  
 SRD Index: 0

4. Configure Proxy Set ID #3 for the IP-PBX:
  - a. From the 'Proxy Set ID' drop-down list, select **3**.
  - b. In the 'Proxy Address' column, enter the IP address of the IP-PBX (e.g., "10.15.4.211").
  - c. From the 'Transport Type' drop-down list corresponding to the IP address entered above, select **UDP**.

- d. In the 'Enable Proxy Keep Alive' drop-down list, select **Using Options**. This is used in Survivability mode for remote IP-PBX users.

**Figure 24-9: Proxy Set ID #3 for the IP-PBX**

The screenshot shows the configuration for Proxy Set ID #3. At the top, a dropdown menu is set to '3'. Below it is a table with 5 rows for Proxy Address and Transport Type. The first row is populated with '10.15.4.211' and 'UDP'. Below the table is a section for Proxy Keep Alive settings. The 'Enable Proxy Keep Alive' dropdown is set to 'Using Options'. Other settings include 'Proxy Keep Alive Time' (60), 'Proxy Load Balancing Method' (Disable), 'Is Proxy Hot Swap' (No), 'Proxy Redundancy Mode' (-1) - Not Configured, and 'SRD Index' (0).

Proxy Address	Transport Type
1 10.15.4.211	UDP
2	
3	
4	
5	

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	(-1) - Not Configured
SRD Index	0

## 24.2.5 Step 5: Configure the IP Groups

This step describes how to create the IP Groups for the following entities in the network:

- ITSP-A SIP trunk
- ITSP-B SIP trunk
- IP-PBX server
- IP-PBX remote users

These IP Groups are later used by the device for routing calls.

### ➤ To configure the IP Groups:

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Define IP Group #1 for ITSP-A:
  - a. From the 'Type' drop-down list, select **Server**.
  - b. In the 'Description' field, type an arbitrary name for the IP Group (e.g., ITSP A).
  - c. From the 'Proxy Set ID' drop-down lists, select **1** (represents the IP addresses, configured in , for communicating with this IP Group).
  - d. In the 'SIP Group Name' field, enter the host name sent in the SIP Request From\To headers for this IP Group, as required by ITSP-A (e.g., RegionA).
  - e. Contact User = name that is sent in the SIP Request's Contact header for this IP Group (e.g., ITSP-A).
3. Define IP Group #2 for ITSP-B:
  - f. From the 'Type' drop-down list, select **Server**.
  - a. In the 'Description' field, type an arbitrary name for the IP Group (e.g., ITSP B).
  - b. From the 'Proxy Set ID' drop-down lists, select **2** (represents the IP addresses, configured in , for communicating with this IP Group).
  - c. In the 'SIP Group Name' field, enter the host name sent in SIP Request From\To headers for this IP Group, as required by ITSP-B (e.g., RegionB).

- d. Contact User = name that is sent in the SIP Request Contact header for this IP Group (e.g., ITSP-B).
4. Define IP Group **#3** for the IP-PBX:
  - a. From the 'Type' drop-down list, select **Server**.
  - b. In the 'Description' field, type an arbitrary name for the IP Group (e.g., IP-PBX).
  - c. From the 'Proxy Set ID' drop-down lists, select **3** (represents the IP address, configured in , for communicating with this IP Group).
  - d. In the 'SIP Group Name' field, enter the host name that is sent in SIP Request From\To headers for this IP Group (e.g., IPPBX).
  - e. Contact User = name that is sent in the SIP Request Contact header for this IP Group (e.g., PBXUSER).
5. Define IP Group **#4** for the remote IP-PBX users:
  - a. From the 'Type' drop-down list, select **User**.
  - b. In the 'Description' field, type an arbitrary name for the IP Group (e.g., IP-PBX).
  - c. In the 'SIP Group Name' field, enter the host name that is used internal in the device's database for this IP Group (e.g., RemoteIPPBXusers).
  - d. From the 'Serving IP Group ID' drop-down list, select **3** (i.e. the IP Group for the IP-PBX).



**Note:** No Serving IP Groups are defined for ITSP-A and ITSP-B. Instead, the Outbound IP Routing table (see 'Step 9: Configure Outbound IP Routing' on page 268) is used to configure outbound IP call routing for calls originating from these ITSP IP Groups.

## 24.2.6 Step 6: Configure the Account Table

The Account table is used by the device to register to an ITSP on behalf of the IP-PBX. As described previously, the ITSP requires registration and authentication to provide service. For the example, the Served IP Group is the IP-PBX (IP Group ID #3) and the Serving IP Groups are the two ITSPs (IP Groups #1 and #2).

### ➤ To configure the Account table:

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).

**Figure 24-10: Defining Accounts for Registration**

Index	Served Trunk Group	Served IP Group	Serving IP Group	Username	Password
2 → 1	-1	3	1	itsp_a	*
3 → 2	-1	3	2	itsp_b	*

Host Name	Register	Contact User	Application Type
2 → regiona	Yes	ITSP-A	Gw\IP2IP
3 → regionb	Yes	ITSP-B	Gw\IP2IP

2. Configure Account ID **#1** for IP-PBX authentication and registration with ITSP-A:
  - In the 'Served IP Group' field, enter "3" to indicate that authentication is performed on behalf of IP Group #3 (i.e., the IP-PBX).
  - In the 'Serving IP Group' field, enter "1" to indicate that registration/authentication is with IP Group #1 (i.e., ITSP-A).

- In the 'Username', enter the SIP username for authentication supplied by ITSP-A (e.g., itsp\_a).
  - In the 'Password' field, enter the SIP password for authentication supplied by ITSP-A (e.g., 12345).
  - In the 'Register' field, enter "1" to enable registration with ITSP-A.
3. Configure Account ID #2 for IP-PBX registration) with ITSP-B Registrar server:
    - In the 'Served IP Group' field, enter "3" to indicate that registration is performed on behalf of IP Group #3 (i.e., the IP-PBX).
    - In the 'Serving IP Group' field, enter "2" to indicate that registration is with IP Group #3 (e.g., ITSP-B).
    - In the 'Username', enter the SIP username for the registration/authentication supplied by ITSP-B (e.g., itsp\_b).
    - In the 'Password' field, enter the SIP password for registration/authentication supplied by ITSP-B (e.g., 11111).
    - In the 'Register' field, enter "1" to enable registration with ITSP-B.

### 24.2.7 Step 7: Configure IP Profiles for Voice Coders

Since different voice coders are used by the IP-PBX (G.711) and the ITSPs (G.723), you need to define two IP Profiles:

- Profile ID #1 - configured with G.711 for the IP-PBX
- Profile ID #2 - configured with G.723 for the ITSPs

These profiles are later used in the Inbound IP Routing table and Outbound IP Routing table.

➤ **To configure IP Profiles for voice coders:**

1. Open the Coder Group Settings page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders Group Settings**)
2. Configure Coder Group ID #1 for the IP-PBX (as shown in the figure below):
  - a. From the 'Coder Group ID' drop-down list, select **1**.
  - b. From the 'Coder Name' drop-down list, select **G.711A-law**.
  - c. Click **Submit**.

**Figure 24-11: Defining Coder Group ID 1**

2a →

Coder Group ID: 1

2b →

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

3. Configure Coder Group ID #2 for the ITSP's (as shown in the figure below):
  - a. From the 'Coder Group ID' drop-down list, select **2**.
  - b. From the 'Coder Name' drop-down list, select **G.723.1**.
  - c. Click **Submit**.

Figure 24-12: Defining Coder Group ID 2

3a → Coder Group ID 2

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
3b → G.723.1	30	5.3	4	Disabled

4. Open the IP Profile Settings page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **IP Profile Settings**).
5. Configure Profile ID #1 for the IP-PBX (as shown below):
  - a. From the 'Profile ID' drop-down list, select **1**.
  - b. From the 'Coder Group' drop-down list, select **Coder Group 1**.
  - c. Click **Submit**.

Figure 24-13: Defining IP Profile ID 1

5a → Profile ID 1  
Profile Name IP-PBX

▼ Common Parameters

RTP IP DiffServ	46
Signaling DiffServ	40
Disconnect on Broken Connection	Yes

5b → Coder Group Coder Group 1

Remote RTP Base UDP Port	0
First Tx DTMF Option	Not Supported
Second Tx DTMF Option	Not Supported
Declare RFC 2833 in SDP	Yes
Add IE In SETUP	
Enable Hold	Enable

6. Configure Profile ID #2 for the ITSP's:
  - a. From the 'Profile ID' drop-down list, select **2**.
  - b. From the 'Coder Group' drop-down list, select **Coder Group 2**.
  - c. Click **Submit**.

## 24.2.8 Step 8: Configure Inbound IP Routing

This step defines how to configure the device for routing inbound (i.e., received) IP-to-IP calls. The table in which this is configured uses the IP Groups that you defined in 'Step 5: Configure the IP Groups' on page 263.



➤ **To configure inbound IP routing:**

1. Open the Inbound IP Routing Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** submenu > **IP to Trunk Group Routing**).

**Figure 24-14: Defining Inbound IP Routing Rules**

<div> <div>Routing Index</div> <div>1-12</div> <div>IP To Tel Routing Mode</div> <div>Route calls before manipulation</div> </div>								
	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IPGroup ID
2	1		9	*	*	1	0	
3	2		*	*	10.15.4.211	-1	1	3
4	3		+1919	*	*	-1	2	1
5	4		0200	*	*	-1	2	2
6	5	pbxremote	*	*	*	-1	0	4
7	6		*	*	10.15.4.211	1	0	-1

2. **Index #1:** routes calls with prefix 9 (i.e., local calls) dialed from IP-PBX users to the local PSTN:
  - 'Dest Phone Prefix': enter "9" for the dialing prefix for local calls.
  - 'Trunk Group ID': enter "1" to indicate that these calls are routed to the Trunk (belonging to Trunk Group #1) connected between the device and the local PSTN network.
3. **Index #2:** identifies IP calls received from the IP-PBX as IP-to-IP calls and assigns them to the IP Group ID configured for the IP-PBX:
  - 'Dest Phone Prefix': enter the asterisk (\*) symbol to indicate all destinations.
  - 'Source IP Address': enter the IP address of the IP-PBX (i.e., 10.15.4.211).
  - 'Trunk Group ID': enter "-1" to indicate that these calls are IP-to-IP calls.
  - 'IP Profile ID': enter "1" to assign these calls to Profile ID #1 to use G.711.
  - 'Source IP Group ID': enter "3" to assign these calls to the IP Group pertaining to the IP-PBX.
4. **Index #3:** identifies IP calls received from ITSP-A as IP-to-IP calls and assigns them to the IP Group ID configured for ITSP-A:
  - 'Dest Phone Prefix': ITSP-A assigns the Enterprise a range of numbers that start with +1919. Enter this prefix to indicate calls received from this ITSP.
  - 'Trunk Group ID': enter "-1" to indicate that these calls are IP-to-IP calls.
  - 'IP Profile ID': enter "2" to assign these calls to Profile ID #2 to use G.723.
  - 'Source IP Group ID': enter "1" to assign these calls to IP Group pertaining to ITSP-A.
5. **Index #4:** identifies IP calls received from ITSP-B as IP-to-IP calls and assigns them to the IP Group ID configured for ITSP-B:
  - 'Dest Phone Prefix': ITSP-B assigns the Enterprise a range of numbers that start with 0200. Enter this prefix to indicate calls coming from this ITSP.
  - 'Trunk Group ID': enter "-1" to indicate that these calls are IP-to-IP calls.
  - 'IP Profile ID': enter "2" to assign these calls to Profile ID #2 to use G.723.
  - 'Source IP Group ID': enter "2" to assign these calls to IP Group pertaining to ITSP-B.

6. **Index #5:** identifies all IP calls received from IP-PBX remote users:
  - 'Source Host Prefix': enter "PBXuser". This is the host name that appears in the From header of the Request URI received from remote IP-PBX users.
  - 'Trunk Group ID': enter "-1" to indicate that these calls are IP-to-IP calls.
  - 'Source IP Group ID': enter "4" to assign these calls to the IP Group pertaining to the remote IP-PBX users.
7. **Index #6:** is used for alternative routing. This configuration identifies all IP calls received from the IP-PBX and which can't reach the ITSP's servers (e.g. loss of connection with ITSP's) and routes them to the local PSTN network:
  - 'Dest Phone Prefix': enter the asterisk (\*) symbol to indicate all destinations.
  - 'Source IP Address': enter the IP address of the IP-PBX (i.e., 10.15.4.211).
  - 'Trunk Group ID': enter "1" to route these calls to the Trunk Group ID configured for the Trunk connected to the device and interfacing with the local PSTN.
  - 'Source IP Group ID': enter "-1" to indicate that these calls are not assigned to any source IP Group.

## 24.2.9 Step 9: Configure Outbound IP Routing

This step defines how to configure the device for routing outbound (i.e., sent) IP-to-IP calls. In our example scenario, calls from both ITSP's must be routed to the IP-PBX, while outgoing calls from IP-PBX users must be routed according to destination. If the calls are destined to the Japanese market, then they are routed to ITSP-B; for all other destinations, the calls are routed to ITSP-A. This configuration uses the IP Groups defined in 'Step 5: Configure the IP Groups' on page 263 and IP Profiles defined in 'Step 7: Configure IP Profiles for Voice Coders' on page 265.

### ➤ To configure outbound IP routing rules:

1. Open the Outbound IP Routing Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **Tel to IP Routing**).
2. Configure **Index #1** to route IP calls received from ITSP-A to the IP-PBX:
  - 'Source IP Group ID': select **1** to indicate received (inbound) calls identified as belonging to the IP Group configured for ITSP-A.
  - 'Dest Phone Prefix' and 'Source Phone Prefix': enter the asterisk (\*) symbol to indicate all destinations and callers respectively.
  - 'Dest IP Group ID': select **3** to indicate the destination IP Group to where these calls are sent, i.e., to the IP-PBX.
  - 'IP Profile ID': enter "2" to indicate the IP Profile configured for G.723.
3. Configure **Index #2** to route IP calls received from ITSP-B to the IP-PBX:
  - 'Source IP Group ID': select **2** to indicate received (inbound) calls identified as belonging to the IP Group configured for ITSP-B.
  - 'Dest Phone Prefix' and 'Source Phone Prefix': enter the asterisk (\*) symbol to indicate all destinations and callers respectively.
  - 'Dest IP Group ID': select **3** to indicate the destination IP Group to where these calls are sent, i.e., to the IP-PBX.
  - 'IP Profile ID': enter "2" to indicate the IP Profile configured for G.723.
4. Configure **Index #3** to route calls received from the local PSTN network to the IP-PBX:
  - 'Source Trunk Group ID': enter "1" to indicate calls received on the trunk connecting the device to the local PSTN network.
  - 'Dest IP Group ID': select **3** to indicate the destination IP Group to where the calls must be sent, i.e., to the IP-PBX.



5. Configure **Index #4** to route IP calls received from the IP-PBX to ITSP-A:
  - 'Source IP Group ID': select **3** to indicate received (inbound) calls identified as belonging to the IP Group configured for the IP-PBX.
  - 'Dest Phone Prefix': enter "+81" to indicate calls to Japan (i.e., with prefix +81).
  - 'Source Phone Prefix': enter the asterisk (\*) symbol to indicate all sources.
  - 'Dest IP Group ID': select **1** to indicate the destination IP Group to where the calls must be sent, i.e., to ITSP-A.
  - 'IP Profile ID': enter "1" to indicate the IP Profile configured for G.711.
6. Configure **Index #5** to route IP calls received from the IP-PBX to ITSP-B:
  - 'Source IP Group ID': select **3** to indicate received (inbound) calls identified as belonging to the IP Group configured for the IP-PBX.
  - 'Dest Phone Prefix' and 'Source Phone Prefix': enter the asterisk (\*) symbol to indicate all destinations (besides Japan) and all sources respectively.
  - 'Dest IP Group ID': select **2** to indicate the destination IP Group to where the calls must be sent, i.e., to ITSP-A.
  - 'IP Profile ID': enter "1" to indicate the IP Profile configured for G.711.
7. Configure **Index #6** to route dialed calls (four digits starting with digit 4) from IP-PBX to remote IP-PBX users. The device searches its database for the remote users registered number, and then sends an INVITE to the remote user's IP address (listed in the database):
  - 'Source IP Group ID': select **3** to indicate received (inbound) calls identified as belonging to the IP Group configured for the IP-PBX.
  - 'Dest Phone Prefix': enter the "4xxx#" to indicate all calls dialed from IP-PBX that include four digits and start with the digit 4.
  - 'Dest IP Group ID': select **4** to indicate the destination IP Group to where the calls must be sent, i.e., to remote IP-PBX users.
  - 'IP Profile ID': enter "1" to indicate the IP Profile configured for G.711.

### 24.2.10 Step 10: Configure Destination Phone Number Manipulation

This step defines how to manipulate the destination phone number. The IP-PBX users in our example scenario use a 4-digit extension number. The incoming calls from the ITSP's have different prefixes and different lengths. This manipulation leaves only the four digits of the user's destination number coming from the ITSP's.

➤ **To configure destination phone number manipulation rules:**

1. Open the Destination Phone Number Manipulation Table for IP -> Tel calls page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Manipulations** > **Dest Number Tel->IP**).
2. Configure Index #1 to manipulate destination number of IP calls received from ITSP-A. The phone number of calls received with prefix +1919 (i.e., from ITSP-A) are removed except for the last four digits:
  - 'Destination Prefix': enter the prefix "+1919".
  - 'Source Prefix': enter the asterisk (\*) symbol to indicate all sources.
  - 'Number of Digits to Leave': enter "4" to leave only the last four digits.

3. Configure Index #2 to manipulate destination number of IP calls received from ITSP-B. The phone number of calls received with prefix 0200 (i.e., from ITSP-B) are removed except for the last four digits:
  - 'Destination Prefix': enter the prefix "0200".
  - 'Source Prefix': enter the asterisk (\*) symbol to indicate all sources.
  - 'Number of Digits to Leave': enter "4" to leave only the last four digits.


## 25 Digital PSTN

This section describes the configuration of the public switched telephone network (PSTN) related parameters.


### 25.1 Configuring Trunk Settings


The Trunk Settings page allows you to configure the device's trunks. This includes selecting the PSTN protocol and configuring related parameters. This page also provides the following features:



- **Taking a Trunk Out of Service:** Some parameters can be configured when the trunk is in service, while others require you to take the trunk out of service. This is done by

clicking the **Stop**  button. Once you have "stopped" a trunk, all current calls are dropped and no new calls can be made on the trunk.

- **Deactivating a Trunk:** You can deactivate a trunk for maintenance. This is done by

clicking the **Deactivate**  button. Deactivation temporarily disconnects (logically) the trunk from the PSTN network. Upon trunk deactivation, the device generates an AIS alarm on the trunk to the far-end. As a result, an RAI alarm signal may be received by the device. A subsequent trunk activation, done by clicking the

**Activate**  button, reconnects the trunk to the PSTN network and clears the AIS alarm. Trunk deactivation is typically used for maintenance such as checking the trunk's physical integrity.

- **Creating a Loopback Line:** You can create (and remove) remote loopback for DS1 lines. This is done by clicking the **Create Loopback**  button. To remove the loopback, click the **Remove Loopback**  button.

For a description of the trunk parameters, see 'PSTN Parameters' on page [799](#).

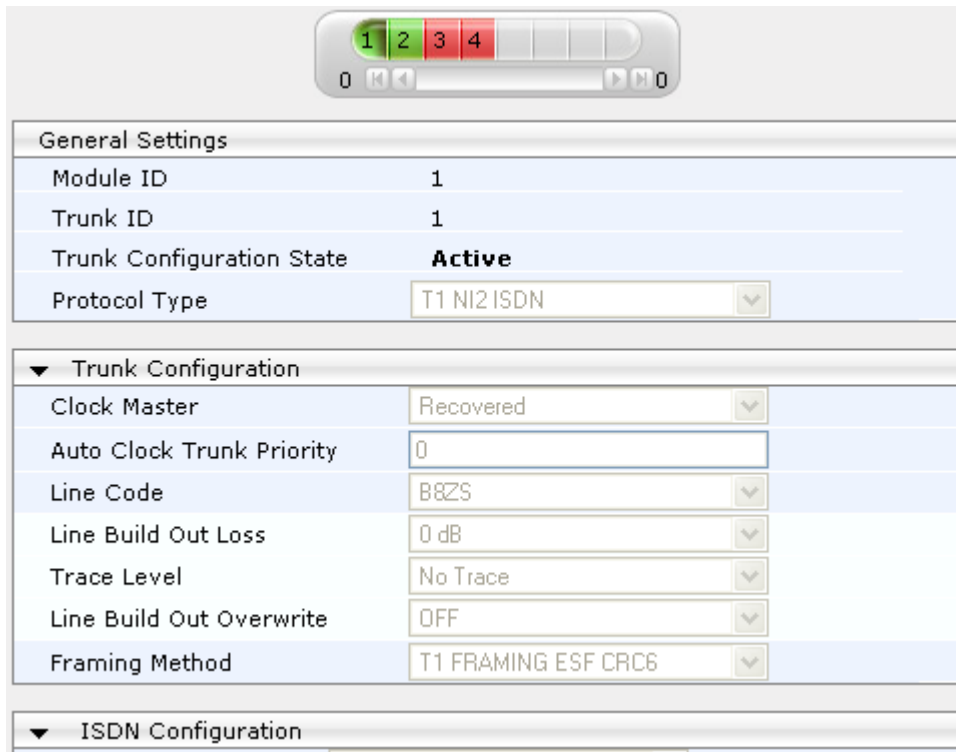


**Notes:**

- During trunk deactivation, trunk configuration cannot be performed.
- A stopped trunk cannot also be activated and a trunk cannot be deactivated if it has been stopped.

➤ **To configure the trunks:**

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



General Settings	
Module ID	1
Trunk ID	1
Trunk Configuration State	<b>Active</b>
Protocol Type	T1 NI2 ISDN

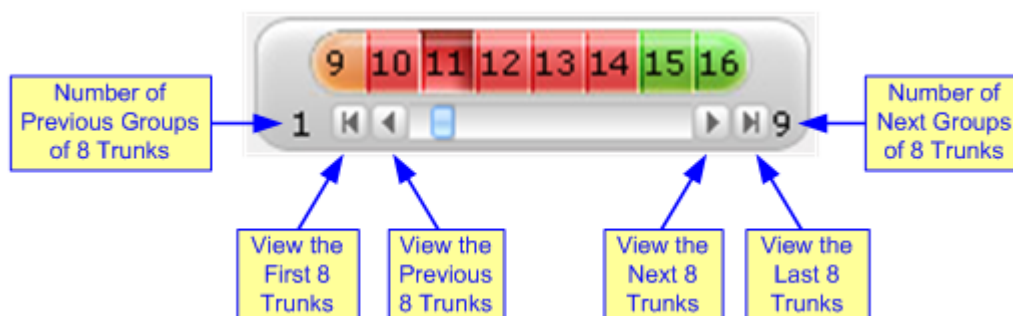
Trunk Configuration	
Clock Master	Recovered
Auto Clock Trunk Priority	0
Line Code	B8ZS
Line Build Out Loss	0 dB
Trace Level	No Trace
Line Build Out Overwrite	OFF
Framing Method	T1 FRAMING ESF CRC6

ISDN Configuration	
--------------------	--

On the top of the page, a bar with Trunk number icons displays the status of each trunk, according to the following color codes:

- **Grey:** Disabled
  - **Green:** Active
  - **Yellow:** RAI alarm (also appears when you deactivate a Trunk by clicking the **Deactivate** button)
  - **Red:** LOS/LOF alarm
  - **Blue:** AIS alarm
  - **Orange:** D-channel alarm (ISDN only)
2. Select the trunk that you want to configure by clicking the desired Trunk number icon. The bar initially displays the first eight trunk number icons (i.e., trunks 1 through 8). To scroll through the trunk number icons (i.e., view the next/last or previous/first group of eight trunks), see the figure below:

**Figure 25-1: Trunk Scroll Bar (Used Only as an Example)**








**Note:** If the Trunk scroll bar displays all available trunks, the scroll bar buttons are unavailable.

After you have selected a trunk, the following is displayed:

- The read-only 'Module ID' field displays the module number to which the trunk belongs.
- The read-only 'Trunk ID' field displays the selected trunk number.
- The read-only 'Trunk Configuration State' displays the state of the trunk ('Active' or 'Inactive').
- The displayed parameters pertain to the selected trunk only.

3. Click the **Stop Trunk**  button (located at the bottom of the page) to take the trunk out of service so that you can configure the currently grayed out (unavailable) parameters. (Skip this step if you want to configure parameters that are available when the trunk is active). The stopped trunk is indicated by the following:

- The 'Trunk Configuration State' field displays 'Inactive'.
- The **Stop Trunk** button is replaced by the **Apply Trunk Settings**  button.

When all trunks are stopped, the **Apply to All Trunks**  button also appears.

- All the parameters are available and can be modified.
4. Configure the trunk parameters as required.
  5. Click the **Apply Trunk Settings** button to apply the changes to the selected trunk (or click **Apply to All Trunks** to apply the changes to all trunks); the **Stop Trunk** button replaces **Apply Trunk Settings** and the 'Trunk Configuration State' displays 'Active'.
  6. To save the changes to flash memory, see 'Saving Configuration' on page 532.
  7. To reset the device, see 'Resetting the Device' on page 529.



**Notes:**

- If the 'Protocol Type' field displays 'NONE' (i.e., no protocol type is selected) and no other trunks have been configured, after selecting a PRI protocol type, you must reset the device.
- The displayed parameters depend on the protocol selected.
- All PRI trunks of the device must be of the same line type (i.e., E1 or T1). However, different variants of the same line type can be configured on different trunks, for example, E1 Euro ISDN and E1 CAS (subject to the constraints in the device's Release Notes).
- BRI trunks can operate with E1 or T1 trunks.
- If the protocol type is CAS, you can assign or modify a dial plan (in the 'Dial Plan' field) and perform this without stopping the trunk.
- If the trunk can't be stopped because it provides the device's clock (assuming the device is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the device's clock or enable 'TDM Bus PSTN Auto Clock' in the TDM Bus Settings page (see 'TDM and Timing' on page 274).
- To delete a previously configured trunk, set the parameter 'Protocol Type' to 'None'.

## 25.2 TDM and Timing

This section describes the configuration of the TDM and clock timing parameters.

### 25.2.1 Configuring TDM Bus Settings

The TDM page allows you to configure the device's Time-Division Multiplexing (TDM) bus settings. For a description of these parameters, see 'PSTN Parameters' on page 799.

➤ To configure the TDM Bus settings:

1. Open the TDM page (**Configuration** tab > **VoIP** menu > TDM > TDM Bus Settings).

TDM Bus Settings	
PCM Law Select	MuLaw
TDM Bus Clock Source	Internal
TDM Bus PSTN Auto FallBack Clock	Disable
TDM Bus PSTN Auto Clock Reverting	Disable
Idle PCM Pattern	255
Idle ABCD Pattern	0x0F
TDM Bus Local Reference	1
TDM Bus Type	Frainers

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. Save the changes to flash memory, see 'Saving Configuration' on page 532.

### 25.2.2 Clock Settings

In a traditional TDM service network such as PSTN, both ends of the TDM connection must be synchronized. If synchronization is not achieved, voice frames are either dropped (to prevent a buffer overflow condition) or inserted (to prevent an underflow condition). In both cases, connection quality and reliability is affected.

- PSTN line clock (see 'Recovering Clock from PSTN Line' on page 275)
- Internal clock (see 'Configuring Internal Clock as Clock Source' on page 275)



**Note:** When the device is used in a 'non-span' configuration, the internal device clock must be used (as explained above).

### 25.2.2.1 Recovering Clock from PSTN Line Interface

This section provides a brief description for configuring synchronization based on recovering clock from the PSTN line (Trunk) interface. For a full description of the clock parameters, see 'PSTN Parameters' on page 799.

➤ **To configure synchronization based on clock from PSTN line:**

1. In the TDM Bus Settings page, do the following:
  - a. Set the 'TDM Bus Clock Source' parameter (TDMBusClockSource) to **Network** to recover the clock from the line interface.
  - b. Select the trunk from which the clock is derived, using the 'TDM Bus Local Reference' parameter (TDMBusLocalReference).



**Note:** The E1/T1 trunk should recover the clock from the remote side (see below description of the 'Clock Master' parameter). The BRI trunk should be configured as an ISDN user-side.

- c. Enable automatic switchover to the next available "salve" trunk if the device detects that the local-reference trunk is no longer capable of supplying the clock to the system:
    1. Set the 'TDM Bus PSTN Auto FallBack Clock' parameter (TDMBusPSTNAutoClockEnable) to **Enable**.
    2. Enable the device to switch back to a previous trunk that returns to service if it has higher switchover priority, using the 'TDM Bus PSTN Auto Clock Reverting' parameter (TDMBusPSTNAutoClockRevertingEnable).
    3. In the Trunk Settings page, configure the priority level of the trunk for taking over as a local-reference trunk, using the 'Auto Clock Trunk Priority' parameter (AutoClockTrunkPriority). A value of 100 means that it never uses the trunk as local reference.
2. For E1/T1 trunks, set the PSTN trunk to recover/derive clock from/to the remote side of the PSTN trunk (i.e. clock slave or clock master): In the Trunk Settings page, set the 'Clock Master' parameter (ClockMaster) to one of the following:
  - **Recovered** - to recover clock (i.e. slave)
  - **Generated** - to transmit clock (i.e. master)

### 25.2.2.2 Configuring Internal Clock as Clock Source

This section describes how to configure the device to use its internal clock source. The internal clock source is a stratum 4E-compliant clock source. When the device has no line interfaces, the device should be configured in this mode.

➤ **To configure internal clock as clock source:**

1. Set the clock source to be from the device's internal oscillator. In the TDM Bus Settings page, set the 'TDM Bus Clock Source' parameter (TDMBusClockSource) to **Internal**.
2. For E1/T1 trunks only, set the line to drive the clock on all trunks: In the Trunk Settings page, set the 'Clock Master' parameter (ClockMaster) to **Generated** (for all trunks).

## 25.3 Configuring CAS State Machines

The CAS State Machine page allows you to modify various timers and other basic parameters to define the initialization of the CAS state machine without changing the state machine itself (no compilation is required). The change doesn't affect the state machine itself, but rather the configuration.

The CAS table used can be chosen in two ways (using the parameter CasChannelIndex):

- Single CAS table per trunk
- Different CAS table per group of B-channels in a trunk



**Note:** The CAS state machine can only be configured using the Web-based management tool.

### ➤ To modify the CAS state machine parameters:

1. Open the CAS State Machine page (**Configuration** tab > **VoIP** menu > **PSTN** submenu > **CAS State Machines**).

**Figure 25-2: CAS State Machine Page**

CAS Table Name	Generate Digit On Time	Generate Inter Digit Time	DTMF Max Detection Time	DTMF Min Detection Time	Max Incoming Address Digits	Max Incoming ANI Digits
E_M_FGDWinkTable.dat	-1	-1	-1	-1	-1	-1
E_M_FGDWinkTable.dat	-1	-1	-1	-1	-1	-1
E_M_FGDWinkTable.dat	-1	-1	-1	-1	-1	-1

2. Ensure that the trunk is inactive. The trunk number displayed in the 'Related Trunks' field must be green. If it is red, indicating that the trunk is active, click the trunk number to open the Trunk Settings page (see 'Configuring Trunk Settings' on page 271), select the required Trunk number icon, and then click **Stop Trunk**.
3. In the CAS State Machine page, modify the required parameters according to the table below.
4. Once you have completed the configuration, activate the trunk if required in the Trunk Settings page, by clicking the trunk number in the 'Related Trunks' field, and in the Trunk Settings page, select the required Trunk number icon, and then click **Apply Trunk Settings**.
5. Click **Submit**, and then reset the device (see 'Resetting the Device' on page 529).



### Notes:

- Don't modify the default values unless you fully understand the implications of the changes and know the default values. Every change affects the configuration of the state machine parameters and the call process related to the trunk you are using with this state machine.
- You can modify CAS state machine parameters only if the following conditions are met:
  - 1) Trunks are inactive (stopped), i.e., the 'Related Trunks' field displays the trunk number in green.
  - 2) State machine is not in use or is in reset, or when it is not related to any trunk. If it is related to a trunk, you must delete the trunk or deactivate (*Stop*) the trunk.
- Field values displaying '-1' indicate CAS default values. In other words, CAS state machine values are used.



- The modification of the CAS state machine occurs at the CAS application initialization only for non-default values (-1).
- For more information on the CAS Protocol table, refer to the *CAS Protocol Table Configuration Note*.

### CAS State Machine Parameters Description

Parameter	Description
Generate Digit On Time <b>[CasStateMachineGenerateDigitOnTime]</b>	Generates digit on-time (in msec). The value must be a positive value. The default is -1 (use value from CAS state machine).
Generate Inter Digit Time <b>[CasStateMachineGenerateInterDigitTime]</b>	Generates digit off-time (in msec). The value must be a positive value. The default is -1 (use value from CAS state machine).
DTMF Max Detection Time <b>[CasStateMachineDTMFMaxOnDetectionTime]</b>	Detects digit maximum on time (according to DSP detection information event) in msec units. The value must be a positive value. The default is -1 (use value from CAS state machine).
DTMF Min Detection Time <b>[CasStateMachineDTMFMinOnDetectionTime]</b>	Detects digit minimum on time (according to DSP detection information event) in msec units. The digit time length must be longer than this value to receive a detection. Any number may be used, but the value must be less than CasStateMachineDTMFMaxOnDetectionTime. The value must be a positive value. The default is -1 (use value from CAS state machine).
MAX Incoming Address Digits <b>[CasStateMachineMaxNumOfIncomingAddressDigits]</b>	Defines the limitation for the maximum address digits that need to be collected. After reaching this number of digits, the collection of address digits is stopped. The value must be an integer. The default is -1 (use value from CAS state machine).
MAX Incoming ANI Digits <b>[CasStateMachineMaxNumOfIncomingANIDigits]</b>	Defines the limitation for the maximum ANI digits that need to be collected. After reaching this number of digits, the collection of ANI digits is stopped. The value must be an integer. The default is -1 (use value from CAS state machine).
Collect ANI <b>[CasStateMachineCollectANI]</b>	In some cases, when the state machine handles the ANI collection (not related to MFCR2), you can control the state machine to collect ANI or discard ANI. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No = Don't collect ANI.</li> <li>▪ <b>[1]</b> Yes = Collect ANI.</li> <li>▪ <b>[-1]</b> Default = Default value - use value from CAS state machine.</li> </ul>
Digit Signaling System <b>[CasStateMachineDigitSignalingSystem]</b>	Defines which Signaling System to use in both directions (detection\generation). <ul style="list-style-type: none"> <li>▪ <b>[0]</b> DTMF = Uses DTMF signaling.</li> <li>▪ <b>[1]</b> MF = Uses MF signaling (default).</li> <li>▪ <b>[-1]</b> Default = Default value - use value from CAS state machine.</li> </ul>

## 25.4 Configuring Digital Gateway Parameters

The Digital Gateway Parameters page allows you to configure miscellaneous digital parameters. For a description of these parameters, see 'Configuration Parameters Reference' on page 661.

➤ **To configure the digital gateway parameters:**

1. Open the Digital Gateway Parameters page (**Configuration** tab > **VoIP** menu > **GW and IP** to **IP** submenu > **Digital Gateway** submenu > **Digital Gateway Parameters**).

**Figure 25-3: Digital Gateway Parameters Page**

B-channel Negotiation	Exclusive
Swap Redirect and Called Numbers	No
MFC R2 Category	1
Disconnect Call on Busy Tone Detection (CAS)	Enable
Disconnect Call on Busy Tone Detection (ISDN)	Disable
Enable TDM Tunneling	Disable
Send Screening Indicator to IP	Not Configured
Send Screening Indicator to ISDN	Not Configured
Add IE in SETUP	
Trunk Groups to Send IE	
Enable User-to-User IE for Tel to IP	Disable
Enable User-to-User IE for IP to Tel	Disable
Enable ISDN Tunneling Tel to IP	Disable
Enable QSIG Tunneling	Disable
Enable ISDN Tunneling IP to Tel	Disable
ISDN Transfer on Connect	Alert
Remove CLI when Restricted	No
Remove Calling Name	Disable
Tdm Over IP Minimum Calls For Trunk Activation	0
ISDN Facility Trace	Disable
Use EndPoint Number As Calling Number Tel2IP	Disable
Use EndPoint Number As Calling Number IP2Tel	Disable
Default Cause Mapping From ISDN to SIP	0
Add Prefix to Redirect Number	
Copy Destination Number to Redirect Number	Don't copy
Enable Calling Party Category	Disable
ISDN SubAddress Format	ASCII
Play Local RBT on ISDN Transfer	Don't play
Send Local Time To ISDN Connect	Disable
User To User Header Format	0
Digital Out-Of-Service Behavior	Default
Ignore BRI LOS Alarm	Enable

MLPP	
MLPP Default Namespace	DSN
Default Call Priority	0
Preemption tone Duration	3
RTP DSCP for MLPP Routine	-1
RTP DSCP for MLPP Priority	-1
RTP DSCP for MLPP Immediate	-1
RTP DSCP for MLPP Flash	-1
RTP DSCP for MLPP Flash-Override	-1
RTP DSCP for MLPP Flash-Override-Override	-1
MLPP Default Service Domain	000000
MLPP Normalized Service Domain	000000

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 25.5 Tunneling Applications

This section discusses the device's support for VoIP tunneling applications.

### 25.5.1 TDM Tunneling

The device's TDM Tunneling feature allows you to tunnel groups of digital trunk spans or timeslots (B-channels) over the IP network. TDM Tunneling utilizes the device's internal routing (without Proxy control) capabilities to receive voice and data streams from TDM (E1/T1/J1) spans or individual timeslots, convert them into packets, and then transmit them over the IP network (using point-to-point or point-to-multipoint device distributions). A device opposite it (or several devices when point-to-multipoint distribution is used) converts the IP packets back into TDM traffic. Each timeslot can be targeted to any other timeslot within a trunk in the opposite device.

When TDM Tunneling is enabled (the parameter `EnableTDMoverIP` is set to '1') on the originating device, the originating device automatically initiates SIP calls from all enabled B-channels belonging to the E1/T1/J1 spans that are configured with the protocol type 'Transparent' (for ISDN trunks) or 'Raw CAS' (for CAS trunks). The called number of each call is the internal phone number of the B-channel from where the call originates. The Inbound IP Routing Table is used to define the destination IP address of the terminating device. The terminating device automatically answers these calls if its E1/T1 protocol type is set to 'Transparent' (`ProtocolType` = 5) or 'Raw CAS' (`ProtocolType` = 3 for T1 and 9 for E1) and the parameter `ChannelSelectMode` is set to 0 (By Phone Number).



**Note:** It's possible to configure both devices to also operate in symmetric mode. To do so, set `EnableTDMoverIP` to 1 and configure the Outbound IP Routing Table in both devices. In this mode, each device (after it's reset) initiates calls to the second device. The first call for each B-channel is answered by the second device.

The device continuously monitors the established connections. If for some reason, one or more calls are released, the device automatically re-establishes these 'broken' connections. When a failure in a physical trunk or in the IP network occurs, the device re-establishes the tunneling connections when the network is restored.



**Note:** It's recommended to use the keep-alive mechanism for each connection, by activating the 'session expires' timeout and using Re-INVITE messages.

The device supports the configuration (`TDMolPInitiateInviteTime` and `TDMolPInviteRetryTime` parameters) of the following timers for the TDM-over-IP tunneling application:

- Time between successive INVITEs sent from the same E1/T1 trunk.
- Time between call release and the new INVITE that is sent on the same channel. The call can be released if the device receives a 4xx or 5xx response.

By utilizing the 'Profiles' mechanism (see 'Coders and Profiles' on page 233), you can configure the TDM Tunneling feature to choose different settings based on a timeslot or groups of timeslots. For example, you can use low-bit-rate vocoders to transport voice and 'Transparent' coder to transport data (e.g., for D-channel). You can also use Profiles to assign ToS (for DiffServ) per source - a timeslot carrying data or signaling is assigned a higher priority value than a timeslot carrying voice.

For tunneling of E1/T1 CAS trunks, set the protocol type to 'Raw CAS' (ProtocolType = 3 / 9) and enable RFC 2833 CAS relay mode ('CAS Transport Type' parameter is set to 'CAS RFC2833 Relay').



**Note:** For TDM over IP, the parameter CallerIDTransportType must be set to '0' (disabled), i.e., transparent.

Below is an example of *ini* files for two devices implementing TDM Tunneling for four E1 spans. Note that in this example both devices are dedicated to TDM tunneling.

#### Terminating Side:

```
EnableTDMOverIP = 1
;E1_TRANSPARENT_31
ProtocolType_0 = 5
ProtocolType_1 = 5
ProtocolType_2 = 5
ProtocolType_3 = 5

[PREFIX]
PREFIX_DestinationPrefix, PREFIX_DestAddress, PREFIX_SourcePrefix,
PREFIX_ProfileId, PREFIX_MeteringCode, PREFIX_DestPort,
PREFIX_SrcIPGroupID, PREFIX_DestHostPrefix, PREFIX_DestIPGroupID,
PREFIX_SrcHostPrefix, PREFIX_TransportType,
PREFIX_SrcTrunkGroupID, PREFIX_DestSRD, PREFIX_CostGroup,
PREFIX_ForkingGroup;
Prefix 1 = *,10.8.24.12;
[\\PREFIX]

;IP address of the device in the opposite
;location
;Channel selection by Phone number.
ChannelSelectMode = 0
;Profiles can be used do define different coders per B-channels
;such as Transparent
;coder for B-channels (timeslot 16) that carries PRI ;signaling.
[TrunkGroup]
FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum,
TrunkGroup_FirstTrunkId, TrunkGroup_LastTrunkId,
TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel,
TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId,
TrunkGroup_Module;
TrunkGroup 1 = 0,0,0,1,31,1000,1;
TrunkGroup 1 = 0,1,1,1,31,2000,1;
TrunkGroup 1 = 0,2,2,1,31,3000,1;
TrunkGroup 1 = 0,3,3,1,31,4000,1;
TrunkGroup 1 = 0,0,0,16,16,7000,2;
TrunkGroup 1 = 0,1,1,16,16,7001,2;
TrunkGroup 1 = 0,2,2,16,16,7002,2;
TrunkGroup 1 = 0,3,3,16,16,7003,2;
[/TrunkGroup]
[ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = g7231;
CodersGroup0 1 = Transparent;
[ \\CodersGroup0 ]
[TelProfile]
FORMAT TelProfile_Index = TelProfile_ProfileName,
```

```

TelProfile_TelPreference, TelProfile_CodersGroupID,
TelProfile_IsFaxUsed, TelProfile_JitterBufMinDelay,
TelProfile_JitterBufOptFactor, TelProfile_IPDiffServ,
TelProfile_SigIPDiffServ, TelProfile_DtmfVolume,
TelProfile_InputGain, TelProfile_VoiceVolume,
TelProfile_EnableReversePolarity,
TelProfile_EnableCurrentDisconnect,
TelProfile_EnableDigitDelivery, TelProfile_EnableEC,
TelProfile_MWIAAnalog, TelProfile_MWIDisplay,
TelProfile_FlashHookPeriod, TelProfile_EnableEarlyMedia,
TelProfile_ProgressIndicator2IP;
TelProfile 1 = voice,$$,1,$$,,$$,,$$,,$$,,$$,,$$;
TelProfile 2 = data,$$,2,$$,,$$,,$$,,$$,,$$,,$$;
[ \TelProfile ]

```

### Originating Side:

```

;E1_TRANSPARENT_31
ProtocolType_0 = 5
ProtocolType_1 = 5
ProtocolType_2 = 5
ProtocolType_3 = 5
;Channel selection by Phone number.
ChannelSelectMode = 0
[ TrunkGroup ]
FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum,
TrunkGroup_FirstTrunkId, TrunkGroup_LastTrunkId,
TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel,
TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId,
TrunkGroup_Module;
TrunkGroup 0 = 0,0,0,1,31,1000,1;
TrunkGroup 0 = 0,1,1,1,31,2000,1;
TrunkGroup 0 = 0,2,2,1,31,3000,1;
TrunkGroup 0 = 0,3,1,31,4000,1;
TrunkGroup 0 = 0,0,0,16,16,7000,2;
TrunkGroup 0 = 0,1,1,16,16,7001,2;
TrunkGroup 0 = 0,2,2,16,16,7002,2;
TrunkGroup 0 = 0,3,3,16,16,7003,2;
[ \TrunkGroup ]
[ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = g7231;
CodersGroup0 1 = Transparent;
[ \CodersGroup0 ]
[ TelProfile ]
FORMAT TelProfile_Index = TelProfile_ProfileName,
TelProfile_TelPreference, TelProfile_CodersGroupID,
TelProfile_IsFaxUsed, TelProfile_JitterBufMinDelay,
TelProfile_JitterBufOptFactor, TelProfile_IPDiffServ,
TelProfile_SigIPDiffServ, TelProfile_DtmfVolume,
TelProfile_InputGain, TelProfile_VoiceVolume,
TelProfile_EnableReversePolarity,
TelProfile_EnableCurrentDisconnect,
TelProfile_EnableDigitDelivery, TelProfile_EnableEC,
TelProfile_MWIAAnalog, TelProfile_MWIDisplay,
TelProfile_FlashHookPeriod, TelProfile_EnableEarlyMedia,
TelProfile_ProgressIndicator2IP;
TelProfile_1 = voice,$$,1,$$,,$$,,$$,,$$,,$$,,$$

```

```
TelProfile_2 = data,$$,2,$$,,$$,,$$,,$$,,$$,,$$
[\TelProfile]
```

### 25.5.1.1 DSP Pattern Detector

For TDM tunneling applications, you can use the DSP pattern detector feature to initiate the echo canceller at call start. The device can be configured to support detection of a specific one-byte idle data pattern transmitted over digital E1/T1 timeslots. The device can be configured to detect up to four different one-byte data patterns. When the defined idle data pattern is detected, the channel resets its echo canceller.

➤ **To configure DSP pattern detector:**

1. In the IPMedia Settings page (**Configuration** tab > **VoIP** menu > **Media** > **IPMedia Settings**), do the following:
  - a. Set the 'IPMedia Detectors' parameter (EnabledDSPIPMDetectors) to **Enable**.
  - b. Set the 'Enable Pattern Detector' parameter (EnablePatternDetector) to **Enable**.
2. Configure the number (e.g., 5) of consecutive patterns to trigger the pattern detection event, using the ini file parameter, PDThreshold.
3. Configure the patterns that can be detected by the Pattern Detector, using the ini file parameter, PDPattern. For example:

```
PDPattern = 84, 85, 212, 213 ; for idle patterns 54, 55, D4
and D5
```

## 25.5.2 QSIG Tunneling

The device supports QSIG tunneling over SIP, according to IETF Internet-Draft draft-elwell-sipping-qsig-tunnel-03 ("Tunnelling of QSIG over SIP") and ECMA-355/ISO/IEC 22535. This is applicable to all ISDN variants. QSIG tunneling can be applied to all calls or to specific calls using IP Profiles.

QSIG tunneling sends all QSIG messages as raw data in corresponding SIP messages using a dedicated message body. This is used, for example, to enable two QSIG subscribers connected to the same or different QSIG PBX to communicate with each other over an IP network. Tunneling is supported in both directions (Tel-to-IP and IP-to-Tel).

The term tunneling means that messages are transferred 'as is' to the remote side without being converted (QSIG > SIP > QSIG). The advantage of tunneling over QSIG-to-SIP interworking is that by using interworking, QSIG functionality can only be partially achieved. When tunneling is used, all QSIG capabilities are supported and the tunneling medium (the SIP network) does not need to process these messages.

QSIG messages are transferred in SIP messages in a separate Multipurpose Internet Mail Extensions (MIME) body. Therefore, if a message contains more than one body (e.g., SDP and QSIG), multipart MIME must be used. The Content-Type of the QSIG tunneled message is 'application/QSIG'. The device also adds a Content-Disposition header in the following format:

```
Content-Disposition: signal; handling=required.
```

QSIG tunneling is done as follows:

- **Call setup (originating device):** The QSIG Setup request is encapsulated in the SIP INVITE message without being altered. After the SIP INVITE request is sent, the device does not encapsulate the subsequent QSIG message until a SIP 200 OK response is received. If the originating device receives a 4xx, 5xx, or 6xx response, it disconnects the QSIG call with a 'no route to destination' cause.
- **Call setup (terminating device):** After the terminating device receives a SIP INVITE request with a 'Content-Type: application/QSIG', it sends the encapsulated QSIG Setup message to the Tel side and sends a 200 OK response (no 1xx response is

sent) to IP. The 200 OK response includes an encapsulated QSIG Call Proceeding message (without waiting for a Call Proceeding message from the Tel side). If tunneling is disabled and the incoming INVITE includes a QSIG body, a 415 response is sent.

- **Mid-call communication:** After the SIP connection is established, all QSIG messages are encapsulated in SIP INFO messages.
- **Call tear-down:** The SIP connection is terminated once the QSIG call is complete. The Release Complete message is encapsulated in the SIP BYE message that terminates the session.

➤ **To enable QSIG tunneling:**

1. In the Digital Gateway Parameters page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Digital Gateway** > **Digital Gateway Parameters**), set the 'Enable QSIG Tunneling' parameter (EnableQSIGTunneling) to **Enable** on the originating and terminating devices.
2. Configure the QSIGTunnelingMode parameter for defining the format of encapsulated QSIG message data in the SIP message MIME body (0 for ASCII presentation; 1 for binary encoding).
3. Set the ISDNDuplicateQ931BuffMode parameter to 128 to duplicate all messages.
4. Set the ISDNInCallsBehavior parameter to 4096.
5. Set the ISDNRxOverlap parameter to 0 for tunneling of QSIG overlap-dialed digits (see below for description).

The configuration of the ISDNInCallsBehavior and ISDNRxOverlap parameters allows tunneling of QSIG overlap-dialed digits (Tel to IP). In this configuration, the device **delays** the sending of the QSIG Setup Ack message upon receipt of the QSIG Setup message. Instead, the device sends the Setup Ack message to QSIG only when it receives the SIP INFO message with Setup Ack encapsulated in its MIME body. The PBX sends QSIG Information messages (to complete the Called Party Number) only after it receives the Setup Ack. The device relays these Information messages encapsulated in SIP INFO messages to the remote party.

## 25.6 ISDN Non-Facility Associated Signaling (NFAS)

In regular T1 ISDN trunks, a single 64 kbps channel carries signaling for the other 23 B-channels of that particular T1 trunk. This channel is called the D-channel and usually resides on timeslot # 24. ISDN Non-Facility Associated Signaling (NFAS) enables the use of a single D-channel to control multiple PRI interfaces.

With NFAS it is possible to define a group of T1 trunks, called an *NFAS group*, in which a single D-channel carries ISDN signaling messages for the entire group. The NFAS group's B-channels are used to carry traffic such as voice or data. The NFAS mechanism also enables definition of a backup D-channel on a different T1 trunk, to be used if the primary D-channel fails.

The device supports up to 12 NFAS groups. Each group can comprise up to 10 T1 trunks and each group must contain different T1 trunks. Each T1 trunk is called an 'NFAS member'. The T1 trunk whose D-channel is used for signaling is called the 'Primary NFAS Trunk'. The T1 trunk whose D-channel is used for backup signaling is called the 'Backup NFAS Trunk'. The primary and backup trunks each carry 23 B-channels while all other NFAS trunks each carry 24 B-channels.

The NFAS group is identified by an NFAS GroupID number (possible values are 1 to 12). To assign a number of T1 trunks to the same NFAS group, use the NFASGroupNumber\_x = groupID (where x is the physical trunk ID (0 to the maximum number of trunks) or the Web interface (see 'Configuring Trunk Settings' on page 271).

The parameter 'DchConfig\_x = Trunk\_type' defines the type of NFAS trunk. Trunk\_type is set to 0 for the primary trunk, to 1 for the backup trunk, and to 2 for an ordinary NFAS



trunk. 'x' denotes the physical trunk ID (0 to the maximum number of trunks). You can also use the Web interface (see 'Configuring Trunk Settings' on page 271).

For example, to assign the first four T1 trunks to NFAS group #1, in which trunk #0 is the primary trunk and trunk #1 is the backup trunk, use the following configuration:

```
NFASGroupNumber_0 = 1
NFASGroupNumber_1 = 1
NFASGroupNumber_2 = 1
NFASGroupNumber_3 = 1
DchConfig_0 = 0           ;Primary T1 trunk
DchConfig_1 = 1           ;Backup T1 trunk
DchConfig_2 = 2           ;24 B-channel NFAS trunk
DchConfig_3 = 2           ;24 B-channel NFAS trunk
```

The NFAS parameters are described in 'PSTN Parameters' on page 799.

## 25.6.1 NFAS Interface ID

Several ISDN switches require an additional configuration parameter per T1 trunk that is called 'Interface Identifier'. In NFAS T1 trunks, the Interface Identifier is sent explicitly in Q.931 Setup / Channel Identification IE for all NFAS trunks, except for the B-channels of the Primary trunk (see note below).

The Interface ID can be defined per member (T1 trunk) of the NFAS group, and must be coordinated with the configuration of the Switch. The default value of the Interface ID is identical to the number of the physical T1 trunk (0 for the first trunk, 1 for the second T1 trunk, and so on, up to the maximum number of trunks).

To define an explicit Interface ID for a T1 trunk (that is different from the default), use the following parameters:

- ISDNIBehavior\_x = 512 (x = 0 to the maximum number of trunks identifying the device's physical trunk)
- ISDNNFASInterfaceID\_x = ID (x = 0 to 255)



### Notes:

- Usually the Interface Identifier is included in the Q.931 Setup/Channel Identification IE only on T1 trunks that doesn't contain the D-channel. Calls initiated on B-channels of the Primary T1 trunk, by default, don't contain the Interface Identifier. Setting the parameter ISDNIBehavior\_x to 2048' forces the inclusion of the Channel Identifier parameter also for the Primary trunk.
- The parameter ISDNNFASInterfaceID\_x = ID can define the 'Interface ID' for any Primary T1 trunk, even if the T1 trunk is not a part of an NFAS group. However, to include the Interface Identifier in Q.931 Setup/Channel Identification IE configure ISDNIBehavior\_x = 2048 in the *ini* file.

## 25.6.2 Working with DMS-100 Switches

The DMS-100 switch requires the following NFAS Interface ID definitions:

- InterfaceID #0 for the Primary trunk
- InterfaceID #1 for the Backup trunk
- InterfaceID #2 for a 24 B-channel T1 trunk
- InterfaceID #3 for a 24 B-channel T1 trunk, and so on for subsequent T1 trunks



For example, if four T1 trunks on a device are configured as a single NFAS group with Primary and Backup T1 trunks that is used with a DMS-100 switch, the following parameters should be used:

```
NFASGroupNumber_0 = 1
NFASGroupNumber_1 = 1
NFASGroupNumber_2 = 1
NFASGroupNumber_3 = 1
DchConfig_0 = 0      ;Primary T1 trunk
DchConfig_1 = 1      ;Backup T1 trunk
DchConfig_2 = 2      ;B-Channel NFAS trunk
DchConfig_3 = 2      ;B-channel NFAS trunk
```

If there is no NFAS Backup trunk, the following configuration should be used:

```
ISDNNFASInterfaceID_0 = 0
ISDNNFASInterfaceID_1 = 2
ISDNNFASInterfaceID_2 = 3
ISDNNFASInterfaceID_3 = 4
ISDNIBehavior = 512    ;This parameter should be added because of
;ISDNNFASInterfaceID configuration above
NFASGroupNumber_0 = 1
NFASGroupNumber_1 = 1
NFASGroupNumber_2 = 1
NFASGroupNumber_3 = 1
DchConfig_0 = 0      ;Primary T1 trunk
DchConfig_1 = 2      ;B-Channel NFAS trunk
DchConfig_2 = 2      ;B-Channel NFAS trunk
DchConfig_3 = 2      ;B-channel NFAS trunk
```

### 25.6.3 Creating an NFAS-Related Trunk Configuration

The procedures for creating and deleting an NFAS group must be performed in the correct order, as described below.

➤ **To create an NFAS Group:**

1. If there's a backup ('secondary') trunk for this group, it must be configured first.
2. Configure the primary trunk before configuring any NFAS ('slave') trunk.
3. Configure NFAS ('slave') trunks.

➤ **To stop / delete an NFAS Group:**

1. Stop or delete (by setting ProtocolType to 0, i.e., 'None') all NFAS ('slave') trunks.
2. Stop or delete (by setting ProtocolType to 0, i.e., 'None') the backup trunk if a backup trunk exists.
3. Stop or delete (by setting ProtocolType to 0, i.e., 'None') the primary trunk.



**Notes:**

- All trunks in the group must be configured with the same values for trunk parameters TerminationSide, ProtocolType, FramingMethod, and LineCode.
- After stopping or deleting the backup trunk, delete the group and then reconfigure it.

## 25.6.4 Performing Manual D-Channel Switchover in NFAS Group

If an NFAS group is configured with two D-channels (Primary and Backup), you can do a manual switchover between these D-channels.

➤ **To manually switchover from active to standby D-channel:**

1. Open the NFAS Group & D-Channel Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **NFAS Group & D-Channel Status**).
2. Select the required NFAS group, and then click the **Switch Activity** button.



### Notes:

- The **Switch Activity** button is unavailable (i.e, grayed out) if a switchover cannot be done due to, for example, alarms or unsuitable states.
- This feature is applicable only to T1 ISDN protocols supporting NFAS, and only if the NFAS group is configured with two D-channels.

## 25.7 ISDN Overlap Dialing

Overlap dialing is a dialing scheme used by several ISDN variants to send and/or receive called number digits one after the other (or several at a time). This is in contrast to en-bloc dialing in which a complete number is sent in one message. ISDN overlap dialing is applicable to PRI and BRI.

The device supports the following ISDN overlap dialing methods:

- Collects ISDN called party number digits and then sends the SIP INVITE to the IP side with the complete destination number (see 'Collecting ISDN Digits and Sending Complete Number in SIP' on page 286)
- Interworks ISDN overlap dialing with SIP, according to RFC 3578 (see 'Interworking ISDN Overlap Dialing with SIP According to RFC 3578' on page 287)

### 25.7.1 Collecting ISDN Digits and Sending Complete Number in SIP

The device can support an overlap dialing mode whereby the device collects the called party number digits from ISDN Q.931 Information messages or DTMF signals, and then sends a SIP INVITE message to the IP side containing the complete destination number.

ISDN overlap dialing for incoming ISDN calls can be configured for the entire device or per E1/T1 trunk. This is configured using the global, `ISDNRxOverlap` parameter or the `ISDNRxOverlap_x` parameter (where x denotes the trunk number), respectively.

By default (see the `ISDNINCallsBehavior` parameter), the device plays a dial tone to the ISDN user side when it receives an empty called number from the ISDN. In this scenario, the device includes the Progress Indicator in the SetupAck ISDN message that it sends to the ISDN side.

The device can also mute in-band DTMF detection until it receives the complete destination number from the ISDN. This is configured using the `MuteDTMFInOverlap` parameter. The Information digits can be sent in-band in the voice stream, or out-of-band using Q.931 Information messages. If Q.931 Information messages are used, the DTMF in-band detector must be disabled. Note that when at least one digit is received in the ISDN Setup message, the device stops playing a dial tone.

The device stops collecting digits (from the ISDN) upon the following scenarios:

- The device receives a Sending Complete IE in the ISDN Setup or Information messages, indicating no more digits.
- The timeout between received digits expires (configured by the TimeBetweenDigits parameter).
- The maximum number of received digits has been reached (configured by the MaxDigits parameter).
- A match is found with the defined digit map (configured by the DigitMapping parameter).

Relevant parameters (described in 'PSTN Parameters' on page 799):

- ISDNRxOverlap\_x = 1 (can be configured per trunk)
- TimeBetweenDigits
- MaxDigits
- MuteDTMFInOverlap
- DigitMapping

For configuring ISDN overlap dialing using the Web interface, see 'Configuring Trunk Settings' on page 271.

## 25.7.2 Interworking ISDN Overlap Dialing with SIP According to RFC 3578

The device supports the interworking of ISDN overlap dialing to SIP and vice versa, according to RFC 3578.

- **Interworking ISDN overlap dialing to SIP (Tel to IP):** The device sends collected digits each time it receives them (initially from the ISDN Setup message and then from subsequent Q.931 Information messages) to the IP side, using subsequent SIP INVITE messages. You can also define the minimum number of overlap digits to collect before sending the first SIP message (INVITE) for routing the call, using the MinOverlapDigitsForRouting parameter.
- **Interworking SIP to ISDN overlap dialing (IP to Tel):** For each received SIP INVITE pertaining to the same dialog session, the device sends an ISDN Setup message (and subsequent Q.931 Information messages) with the collected digits to the Tel side. For all subsequent INVITEs received, the device sends a SIP 484 "Address Incomplete" response to the IP in order to maintain the current dialog session and to receive additional digits from subsequent INVITEs.

Relevant parameters (described in 'PSTN Parameters' on page 799):

- ISDNRxOverlap = 2
- ISDNTxOverlap
- ISDNOutCallsBehavior = 2
- MinOverlapDigitsForRouting
- TimeBetweenDigits
- MaxDigits
- DigitMapping
- MuteDTMFInOverlap

For configuring ISDN overlap dialing using the Web interface, see 'Configuring Trunk Settings' on page 271.

## 25.8 Redirect Number and Calling Name (Display)

The following tables define the device's redirect number and calling name (Display) support for various ISDN variants according to NT (Network Termination) / TE (Termination Equipment) interface direction:

**Calling Name (Display)**

NT/TE Interface	DMS-100	NI-2	4/5ESS	Euro ISDN	QSIG
NT-to-TE	Yes	Yes	Yes	Yes	Yes
TE-to-NT	Yes	Yes	Yes	No	Yes

**Redirect Number**

NT/TE Interface	DMS-100	NI-2	4/5ESS	Euro ISDN	QSIG
NT-to-TE	Yes	Yes	Yes	Yes	Yes
TE-to-NT	Yes	Yes	Yes	Yes*	Yes

\* When using ETSI DivertingLegInformation2 in a Facility IE (not Redirecting Number IE).

## 26 Trunk Group

This section describes the configuration of the device's channels, which entails assigning them numbers and Trunk Group IDs.

### 26.1 Configuring Trunk Group Table

The Trunk Group Table page allows you to define up to 120 Trunk Groups. A Trunk Group is a logical group of physical trunks and channels that are assigned a Trunk Group ID. The Trunk Group can include multiple trunks and ranges of channels.

To enable and activate the channels of the device, Trunk Groups need to be defined and with telephone numbers. Channels that are not defined in this table are disabled. The Trunk Groups are later used for routing IP-to-Tel and Tel-to-IP calls.



#### Notes:

- After you have configured a Trunk Group, you must configure the Inbound IP Routing Table rules (see 'Configuring Inbound IP Routing Table' on page 330) to route incoming IP calls to the Trunk Group. If you do not configure this, calls cannot be established.
- To select the method on how incoming calls are routed to channels within a Trunk Group, see 'Configuring Hunt Group Settings' on page 291.
- The Trunk Group Table can also be configured using the table ini file parameter, TrunkGroup\_x to (see 'Number Manipulation Parameters' on page 859) or CLI command, configure voip> gw hunt-or-trunk-group trunk-group.

#### ➤ To configure the Trunk Group Table:

1. Open the Trunk Group Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Trunk Group** > **Trunk Group**).

Add Phone Context As Prefix		Disable					
Trunk Group Index		1-12					

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 PRI	1	1	1-30	6000	1	1
2	Module 1 PRI	2	2	1-30	7000	2	1
3	Module 2 FXS			1-4	101	3	2
4							

2. Configure the Trunk Group as required. For a description of the parameters, see the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to the flash memory, see 'Saving Configuration' on page 532.
5. To register the Trunk Groups, click the **Register** button. To unregister the Trunk Groups, click **Unregister**. The registration method for each Trunk Group is according to the 'Registration Mode' parameter in the Trunk Group Settings page (see 'Configuring Hunt Group Settings' on page 291).

### Trunk Group Table Parameters

Parameter	Description
Module CLI: module [TrunkGroup_Module]	Defines the module (i.e., FXS, FXO, PRI, or BRI) for which you want to define the Trunk Group.
From Trunk CLI: first-trunk-id [TrunkGroup_FirstTrunkId]	Defines the starting physical Trunk number in the Trunk Group. The number of listed Trunks depends on the device's hardware configuration. <b>Note:</b> This parameter is applicable only to PRI and BRI modules.
To Trunk CLI: last-trunk-id [TrunkGroup_LastTrunkId]	Defines the ending physical Trunk number in the Trunk Group. The number of listed Trunks depends on the device's hardware configuration. <b>Note:</b> This parameter is applicable only to PRI and BRI modules.
Channels CLI: first-b-channel [TrunkGroup_FirstBChannel] CLI: last-b-channel [TrunkGroup_LastBChannel]	Defines the device's channels/ports (analog module) or Trunk B-channels (digital module). To enable channels, enter the channel numbers. You can enter a range of channels by using the syntax <i>n-m</i> , where <i>n</i> represents the lower channel number and <i>m</i> the higher channel number. For example, "1-4" specifies channels 1 through 4. <b>Notes:</b> <ul style="list-style-type: none"> <li>The number of defined channels must not exceed the maximum number of the Trunk's B-channels.</li> <li>To represent all the Trunk's B-channels, enter a single asterisk (*).</li> </ul>
Phone Number CLI: first-phone-number [TrunkGroup_FirstPhoneNumber]	Defines the telephone number(s) of the channels. The valid value can be up to 50 characters. For a range of channels, enter only the first telephone number. Subsequent channels are assigned the next consecutive telephone number. For example, if you enter 400 for channels 1 to 4, then channel 1 is assigned phone number 400, channel 2 is assigned phone number 401, and so on. These numbers are also used for channel allocation for IP-to-Tel calls if the Trunk Group's 'Channel Select Mode' parameter is set to <b>By Dest Phone Number</b> . <b>Notes:</b> <ul style="list-style-type: none"> <li>If this field includes alphabetical characters and the phone number is defined for a range of channels (e.g., 1-4), then the phone number must end with a number (e.g., 'user1').</li> <li>This field is optional for BRI/PRI interfaces. The logical numbers defined in this field are used when an incoming PSTN/PBX call doesn't contain the calling number or called number (the latter being determined by the ReplaceEmptyDstWithPortNumber parameter). These numbers are used to replace them.</li> </ul>
Trunk Group ID CLI: trunk-group-id [TrunkGroup_TrunkGroupNum]	Defines the Trunk Group ID for the specified channels. The same Trunk Group ID can be assigned to more than one group of channels. If an IP-to-Tel call is assigned to a Trunk Group, the IP call is routed to the channel(s) pertaining to that Trunk Group ID. The valid value can be 0 to 119.
Tel Profile ID CLI: tel-profile-id [TrunkGroup_ProfileId]	Assigns a Tel Profile ID to the Trunk Group. <b>Note:</b> For configuring Tel Profiles, see 'Configuring Tel Profiles' on page 237.

## 26.2 Configuring Hunt Group Settings

The Hunt Group Settings allows you to configure the following per Trunk Group:

- Channel select method by which IP-to-Tel calls are assigned to the Trunk Group's channels.
- Registration method for registering Trunk Groups to selected Serving IP Group IDs.



### Notes:

- For configuring Trunk Groups, see Configuring Trunk Group Table on page 289.
- The Hunt Group Settings table can also be configured using the table ini file parameter, TrunkGroupSettings (see 'Number Manipulation Parameters' on page 859) or CLI command, configure voip/gw hunt-or-trunk-group trunk-group-setting.

### ➤ To configure the Hunt Group Settings table:

1. Open the Hunt Group Settings page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Trunk Group** > **Hunt Group Settings**).

Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User	MWI Interrogation Type
1						Not Configured
2						Not Configured
3						Not Configured
4						Not Configured
5						Not Configured
6						Not Configured
7						Not Configured
8						Not Configured
9						Not Configured
10						Not Configured

2. From the 'Index' drop-down list, select the range of entries that you want to edit.
3. Configure the Trunk Group as required. For a description of the parameters, see the table below.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 532.

### Hunt Group Settings Parameters Description

Parameter	Description
Trunk Group ID CLI: trunk-group-id [TrunkGroupSettings_TrunkGroupId]	Defines the Trunk Group ID that you want to configure.

Parameter	Description
Channel Select Mode CLI: channel-select-mode <b>[TrunkGroupSettings_ChannelSelectMode]</b>	<p>Defines the method by which IP-to-Tel calls are assigned to the channels of the Trunk Group.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> By Dest Phone Number = The channel is selected according to the called (destination) number. If the number is not located, the call is released. If the channel is unavailable (e.g., busy), the call is put on call waiting (if call waiting is enabled and no other call is on call waiting); otherwise, the call is released.</li> <li>▪ <b>[1]</b> Cyclic Ascending = The next available channel in the Trunk Group, in ascending cyclic order is selected. After the device reaches the highest channel number in the Trunk Group, it selects the lowest channel number in the Trunk Group, and then starts ascending again.</li> <li>▪ <b>[2]</b> Ascending = The lowest available channel in the Trunk Group is selected, and if unavailable, the next higher channel is selected.</li> <li>▪ <b>[3]</b> Cyclic Descending = The next available channel in descending cyclic order is selected. The next lower channel number in the Trunk Group is always selected. When the device reaches the lowest channel number in the Trunk Group, it selects the highest channel number in the Trunk Group, and then starts descending again.</li> <li>▪ <b>[4]</b> Descending = The highest available channel in the Trunk Group is selected, and if unavailable, the next lower channel is selected.</li> <li>▪ <b>[5]</b> Dest Number + Cyclic Ascending = The channel is selected according to the called number. If the called number isn't found, the next available channel in ascending cyclic order is selected. <b>Note:</b> If the called number is located, but the port associated with the number is busy, the call is released.</li> <li>▪ <b>[6]</b> By Source Phone Number = The channel is selected according to the calling number.</li> <li>▪ <b>[7]</b> Trunk Cyclic Ascending = The channel from the first channel of the next trunk (adjacent to the trunk from which the previous channel was selected) is selected. This option is applicable only to digital interfaces.</li> <li>▪ <b>[8]</b> Trunk &amp; Channel Cyclic Ascending = The device implements the Trunk Cyclic Ascending and Cyclic Ascending methods to select the channel. This method selects the next physical trunk in the Trunk Group, and then selects the B-channel of this trunk according to the Cyclic Ascending method (i.e., selects the channel after the last allocated channel). This option is applicable only to digital interfaces. For example, if the Trunk Group includes two physical trunks, 0 and 1: <ul style="list-style-type: none"> <li>✓ For the first incoming call, the first channel of Trunk 0 is selected.</li> <li>✓ For the second incoming call, the first channel of Trunk 1 is selected.</li> <li>✓ For the third incoming call, the second channel of Trunk 0 is selected.</li> </ul> </li> <li>▪ <b>[9]</b> Ring to Hunt Group = The device allocates IP-to-Tel calls to all the FXS ports (channels) in the Hunt Group. When a call is received for the Hunt Group, all telephones connected to the FXS ports belonging to the Hunt Group start ringing. The call is eventually received by whichever telephone first answers the call (after which the other phones stop ringing). This option is</li> </ul>



Parameter	Description
	<p>applicable only to FXS interfaces.</p> <ul style="list-style-type: none"> <li>▪ <b>[10]</b> Select Trunk by ISDN SuppServ Table = The BRI port/module is selected according to the settings in the ISDN Supplementary Services table (see Configuring ISDN BRI Supplementary Services on page 386), allowing the routing of IP-to-Tel calls to specific BRI endpoints.</li> <li>▪ <b>[11]</b> Dest Number + Ascending = The device allocates a channels to incoming IP-to-Tel calls as follows: <ul style="list-style-type: none"> <li>a. The device attempts to route the call to the channel that is associated with the destination (called) number. If located, the call is sent to that channel.</li> <li>b. If the number is not located or the channel is unavailable (e.g., busy), the device searches in ascending order for the next available channel in the Trunk Group. If located, the call is sent to that channel.</li> <li>c. If all the channels are unavailable, the call is released.</li> </ul> </li> </ul> <p><b>Note:</b> If this parameter is not configured for the Trunk Group, then its channel select method is according to the global parameter, ChannelSelectMode.</p>
Registration Mode CLI: registration-mode <b>[TrunkGroupSettings_RegistrationMode]</b>	<p>Defines the registration method for the Trunk Group:</p> <ul style="list-style-type: none"> <li>▪ <b>[1]</b> Per Gateway = (Default) Single registration for the entire device. This is applicable only if a default Proxy or Registrar IP is configured and Registration is enabled (i.e., parameter IsRegisterUsed is set to 1). In this mode, the SIP URI user part in the From, To, and Contact headers is set to the value of the global registration parameter, GWRegistrationName or username if GWRegistrationName is not configured.</li> <li>▪ <b>[0]</b> Per Endpoint = Each channel in the Trunk Group registers individually. The registrations are sent to the 'Serving IP Group ID' if defined in the table, otherwise, it is sent to the default Proxy, and if no default Proxy, then to the Registrar IP.</li> <li>▪ <b>[4]</b> Don't Register = No registrations are sent by endpoints pertaining to the Trunk Group. For example, if the device is configured globally to register all its endpoints (using the parameter ChannelSelectMode), you can exclude some endpoints from being registered by assigning them to a Trunk Group and configuring the Trunk Group registration mode to 'Don't Register'.</li> <li>▪ <b>[5]</b> Per Account = Registrations are sent (or not) to an IP Group, according to the settings in the Account table (see 'Configuring Account Table' on page 219).</li> </ul> <p>An example is shown below of a REGISTER message for registering endpoint "101" using the registration Per Endpoint mode:</p> <pre>REGISTER sip:SipGroupName SIP/2.0 Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac862428454 From: &lt;sip:101@GatewayName&gt;;tag=1c862422082 To: &lt;sip:101@GatewayName&gt; Call-ID: 9907977062512000232825@10.33.37.78 CSeq: 3 REGISTER Contact: &lt;sip:101@10.33.37.78&gt;;expires=3600 Expires: 3600 User-Agent: Sip-Gateway/v.6.60A.011.002 Content-Length: 0</pre>

Parameter	Description
	<p>The "SipGroupName" in the Request-URI is configured in the IP Group table (see 'Configuring IP Groups' on page 204).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If this parameter is not configured, the registration is performed according to the global registration parameter, ChannelSelectMode.</li> <li>▪ To enable Trunk Group registration, set the global parameter, IsRegisterNeeded to 1. This is unnecessary for 'Per Account' registration mode.</li> <li>▪ If the device is configured globally to register Per Endpoint and an channel group includes four channels to register Per Gateway, the device registers all channels except the first four channels. The group of these four channels sends a single registration request.</li> </ul>
Serving IP Group ID CLI: serving-ip-group <b>[TrunkGroupSettings_ServingIPGroup]</b>	<p>Assigns an IP Group to where INVITE messages received from this Trunk Group are sent. The actual destination to where these INVITE messages are sent is according to the Proxy Set ID associated with the IP Group. The Request-URI host name in the INVITE and REGISTER messages (except for 'Per Account' registration modes) is set to the value of the 'SIP Group Name' parameter configured in the IP Group table (see 'Configuring IP Groups' on page 204).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If this parameter is not configured, the INVITE messages are sent to the default Proxy or according to the Outbound IP Routing Table (see 'Configuring Outbound IP Routing Table' on page 321).</li> <li>▪ If the PreferRouteTable parameter is set to 1 (see 'Configuring Proxy and Registration Parameters' on page 222), the routing rules in the Outbound IP Routing table take precedence over the selected Serving IP Group ID.</li> </ul>
Gateway Name CLI: gateway-name <b>[TrunkGroupSettings_GatewayName]</b>	<p>Defines the host name for the SIP From header in INVITE messages and for the From/To headers in REGISTER requests.</p> <p><b>Note:</b> If this parameter is not configured, the global parameter, SIPGatewayName is used.</p>
Contact User CLI: contact-user <b>[TrunkGroupSettings_ContactUser]</b>	<p>Defines the user part for the SIP Contact URI in INVITE messages and for the From, To, and Contact headers in REGISTER requests.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only if the 'Registration Mode' parameter is set to 'Per Account' and registration through the Account table is successful.</li> <li>▪ If registration fails, the user part in the INVITE Contact header is set to the source party number.</li> <li>▪ The 'Contact User' parameter in the Account table overrides this parameter (see 'Configuring Account Table' on page 219).</li> </ul>

Parameter	Description
Trunk Group Name CLI: trunk-group-name <b>[TrunkGroupSettings_TrunkGroupName]</b>	<p>Defines a name for the Trunk Group. This name represents the Trunk Group in the SIP 'tgrp' parameter of the outgoing INVITE messages (according to RFC 4904). For example:</p> <pre>sip:+16305550100;tgrp=<b>TG-1</b>;trunk-context=+1-630@isp.example.net;user=phone</pre> <p>The valid value can be a string of up to 20 characters. By default, no name is configured.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If this parameter is not configured, the Trunk Group decimal number is used in the SIP 'tgrp' parameter.</li> <li>▪ This feature is enabled by any of the following parameters: <ul style="list-style-type: none"> <li>✓ UseSIPtgrp</li> <li>✓ UseBroadsoftDTG</li> </ul> </li> <li>▪ Currently, this parameter can only be configured using the ini file.</li> </ul>
MWI Interrogation Type CLI: mwi-interrogation-type <b>[TrunkGroupSettings_MWIInterrogationType]</b>	<p>Defines MWI QSIG-to-IP interworking for interrogating MWI supplementary services:</p> <ul style="list-style-type: none"> <li>▪ <b>[255]</b> Not Configured</li> <li>▪ <b>[0]</b> None = Disables the feature.</li> <li>▪ <b>[1]</b> Use Activate Only = MWI Interrogation messages are not sent and only "passively" responds to MWI Activate requests from the PBX.</li> <li>▪ <b>[2]</b> Result Not Used = MWI Interrogation messages are sent, but the result is not used. Instead, the device waits for MWI Activate requests from the PBX.</li> <li>▪ <b>[3]</b> Use Result = MWI Interrogation messages are sent, its results are used, and the MWI Activate requests are used. MWI Activate requests are interworked to SIP NOTIFY MWI messages. The SIP NOTIFY messages are sent to the IP Group defined by the NotificationIPGroupID parameter.</li> </ul> <p><b>Note:</b> This parameter appears in the table only if the VoiceMailInterface parameter is set to 3 (QSIG). Configuring Voice Mail on page <a href="#">389</a>.</p>

## Reader's Notes

## 27 Manipulation

This section describes the configuration of various manipulation processes.

### 27.1 Configuring General Settings

The General Settings page allows you to configure general manipulation parameters. For a description of the parameters appearing on this page, see 'Configuration Parameters Reference' on page 661.

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

1. Open the General Settings page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** submenu > **General Settings**).

**Figure 27-1: General Settings Page**

Set TEL-to-IP Redirect Reason	Not Configured	▼
Set IP-to-TEL Redirect Reason	Not Configured	▼
Redirect number SI to TEL	Not Configured	▼

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.

### 27.2 Configuring Source/Destination Number Manipulation Rules

You can configure rules for manipulating destination and/or source telephone numbers for IP-to-Tel and Tel-to-IP calls. The following number manipulation tables are used for this:

■ **Tel-to-IP calls:**

- Destination Phone Number Manipulation Table for Tel > IP Calls table (up to 120 entries)
- Source Phone Number Manipulation Table for Tel > IP Calls table (up to 120 entries)

■ **IP-to-Tel calls:**

- Destination Phone Number Manipulation Table for IP > Tel Calls table (up to 120 entries)
- Source Phone Number Manipulation Table for IP > Tel Calls table (up to 120 entries)

The number manipulation tables provide two configuration areas:

- Matching characteristics (*Rule*) of incoming call, for example, prefix of destination number.
- Manipulation operation (*Action*), for example, remove user-defined number of digits from the left of the number.

If the incoming call matches the characteristics of a rule, then its manipulation action is applied.

The device searches a matching manipulation rule starting from the first entry (i.e., top of the table). In other words, a rule at the top of the table takes precedence over a rule defined lower down in the table. Therefore, define more specific rules above more generic rules. For example, if you enter 551 in Index 1 and 55 in Index 2, the device applies rule 1 to numbers that start with 551 and applies rule 2 to numbers that start with 550, 552, 553,

and so on until 559. However, if you enter 55 in Index 1 and 551 in Index 2, the device applies rule 1 to all numbers that start with 55, including numbers that start with 551.

You can perform a second "round" (additional) of destination (NumberMapIP2Tel parameter) and source (SourceNumberMapIP2Tel parameter) number manipulations for IP-to-Tel calls on an already manipulated number. The initial and additional number manipulation rules are both configured in these tables. The additional manipulation is performed on the initially manipulated number. Therefore, for complex number manipulation schemes, you only need to configure relatively few manipulation rules in these tables (that would otherwise require many rules). This feature is enabled using the following parameters:

- PerformAdditionalIP2TELSrcManipulation for source number manipulation
- PerformAdditionalIP2TELDestinationManipulation for destination number manipulation

Telephone number manipulation can be useful, for example, for the following:

- Stripping or adding dialing plan digits from or to the number, respectively. For example, a user may need to first dial 9 before dialing the phone number to indicate an external line. This number 9 can then be removed by number manipulation before the call is setup.
- Allowing or blocking Caller ID information according to destination or source prefixes. For more information on Caller ID, see [Configuring Caller Display Information](#) on page 398.
- For digital modules only: Assigning Numbering Plan Indicator (NPI) and Type of Numbering (TON) to IP-to-Tel calls. The device can use a single global setting for NPI/TON classification or it can use the setting in the manipulation tables on a call-by-call basis.



#### Notes:

- Number manipulation can occur before or after a routing decision is made. For example, you can route a call to a specific Trunk Group according to its original number, and then you can remove or add a prefix to that number before it is routed. To determine when number manipulation is performed, configure the 'IP to Tel Routing Mode' parameter (RouteModelIP2Tel) described in 'Configuring Inbound IP Routing Table' on page 330, and 'Tel to IP Routing Mode' parameter (RouteModeTel2IP) described in 'Configuring Outbound IP Routing Table' on page 321.
- The device manipulates the number in the following order: 1) strips digits from the left of the number, 2) strips digits from the right of the number, 3) retains the defined number of digits, 4) adds the defined prefix, and then 5) adds the defined suffix.
- The source/destination number manipulation tables can also be configured using the ini file and CLI:
  - 1) **Destination Phone Number Manipulation Table for IP > Tel Calls table:** NumberMapIP2Tel (ini); configure voip/gw manipulations dst-number-map-ip2tel (CLI)
  - 2) **Destination Phone Number Manipulation Table for Tel > IP Calls table:** NumberMapTel2IP (ini); configure voip/gw manipulations dst-number-map-tel2ip (CLI)
  - 3) **Source Phone Number Manipulation Table for IP > Tel Calls table:** SourceNumberMapIP2Tel (ini); configure voip/gw manipulations src-number-map-ip2tel (CLI)
  - 4) **Source Phone Number Manipulation Table for Tel > IP Calls table:** SourceNumberMapTel2IP (ini); configure voip/gw manipulations src-number-map-tel2ip (CLI)

➤ **To configure number manipulation rules:**

1. Open the required Number Manipulation page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** submenu > **Dest Number IP->Tel**, **Dest Number Tel->IP**, **Source Number IP->Tel**, or **Source Number Tel->IP**); the relevant Manipulation table page is displayed.
2. Click the **Add** button; the following dialog box appears:

**Figure 27-2: Number Manipulation Table - Add Dialog Box**

3. Click the **Rule** tab, and then configure the matching characteristics. For a description of the parameters, see the table below.
4. Click the **Action** tab, and then configure the manipulation operation. For a description of the parameters, see the table below.
5. Click **Submit** to apply your changes.
6. To save the changes to flash memory, see 'Saving Configuration' on page 532.

The table below shows configuration examples of Tel-to-IP source phone number manipulation rules, where:

- **Rule 1:** When the destination number has the prefix 03 (e.g., 035000), source number prefix 201 (e.g., 20155), and from source IP Group ID 2, the source number is changed to, for example, 97120155.
- **Rule 2:** When the source number has prefix 1001 (e.g., 1001876), it is changed to 587623.
- **Rule 3:** When the source number has prefix 123451001 (e.g., 1234510012001), it is changed to 20018.
- **Rule 4:** When the source number has prefix from 30 to 40 and a digit (e.g., 3122), it is changed to 2312.
- **Rule 5:** When the destination number has the prefix 6, 7, or 8 (e.g., 85262146), source number prefix 2001, it is changed to 3146.

Parameter	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5
Source IP Group	2	0	-	-	-
Destination Prefix	03		*	*	[6,7,8]

Parameter	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5
Source Prefix	201	1001	123451001#	[30-40]x	2001
Stripped Digits from Left	-	4	-	-	5
Stripped Digits from Right	-	-	-	1	-
Prefix to Add	971	5	-	2	3
Suffix to Add	-	23	8	-	-
Number of Digits to Leave	-	-	4	-	-
Presentation	Allowed	Restricted	-	-	-

### Number Manipulation Parameters Description

Parameter	Description
<b>Matching Characteristics (Rule)</b>	
Web: Destination Prefix EMS: Prefix CLI: dst-prefix <b>[DestinationPrefix]</b>	Defines the destination (called) telephone number prefix and/or suffix. You can use special notations for denoting the prefix. For example, <b>[100-199](100,101,105)</b> denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. You can also use the \$ sign to denote calls without a called number. For a description of available notations, see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 659.
Web/EMS: Source Prefix CLI: src-prefix <b>[SourcePrefix]</b>	Defines the source (calling) telephone number prefix and/or suffix. You can use special notations for denoting the prefix. For example, <b>[100-199](100,101,105)</b> denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. You can also use the \$ sign to denote calls without a calling number. For a description of available notations, see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 659.
Web/EMS: Source IP Address CLI: src-ip-address <b>[SourceAddress]</b>	Defines the source IP address of the caller. This is obtained from the Contact header in the INVITE message. <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to the number manipulation tables for IP-to-Tel calls.</li> <li>The source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 to 10.8.8.99.</li> <li>The source IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all IP addresses between 10.8.8.0 and 10.8.8.255.</li> </ul>
Web: Source Host Prefix CLI: src-host-prefix <b>[SrcHost]</b>	Defines the URI host name prefix of the incoming SIP INVITE message in the From header. <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to the number manipulation tables for IP-to-Tel calls.</li> <li>The asterisk (*) wildcard can be used to denote any prefix.</li> <li>If the P-Asserted-Identity header is present in the incoming INVITE</li> </ul>



Parameter	Description
	message, then the value of this parameter is compared to the P-Asserted-Identity URI host name (instead of the From header).
Web: Destination Host Prefix CLI: dst-host-prefix <b>[DestHost]</b>	Defines the Request-URI host name prefix of the incoming SIP INVITE message. <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to the number manipulation tables for IP-to-Tel calls.</li> <li>The asterisk (*) wildcard can be used to denote any prefix.</li> </ul>
Web: Source Trunk Group CLI: src-trunk-group-id <b>[SrcTrunkGroupID]</b>	Defines the source Trunk Group ID for Tel-to-IP calls. To denote all Trunk Groups, leave this field empty. <b>Notes:</b> <ul style="list-style-type: none"> <li>The value -1 indicates that this field is ignored in the rule.</li> <li>This parameter is applicable only to the number manipulation tables for Tel-to-IP calls.</li> <li>For IP-to-IP call routing, this parameter is not required (i.e., leave the field empty).</li> </ul>
Web: Source IP Group CLI: src-ip-group-id <b>[SrcIPGroupID]</b>	Defines the IP Group from where the IP call originated. Typically, the IP Group of an incoming INVITE is determined or classified using the Inbound IP Routing Table. If not used (i.e., any IP Group), leave the field empty. <b>Notes:</b> <ul style="list-style-type: none"> <li>The value -1 indicates that this field is ignored.</li> <li>This parameter is applicable only to the number manipulation tables for Tel-to-IP calls.</li> <li>If this Source IP Group has a Serving IP Group, then all calls from this Source IP Group are sent to the Serving IP Group. In this scenario, this table is used only if the PreferRouteTable parameter is set to 1.</li> </ul>
Web: Destination IP Group CLI: dst-ip-group-id <b>[DestIPGroupID]</b>	Defines the IP Group to where the call is sent. <b>Notes:</b> <ul style="list-style-type: none"> <li>The value -1 indicates that this field is ignored.</li> <li>This parameter is applicable only to the Destination Phone Number Manipulation Table for Tel -&gt; IP Calls.</li> </ul>
<b>Operation (Action)</b>	
Web: Stripped Digits From Left EMS: Number Of Stripped Digits CLI: remove-from-left <b>[RemoveFromLeft]</b>	Defines the number of digits to remove from the left of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 1234.
Web: Stripped Digits From Right EMS: Number Of Stripped Digits CLI: remove-from-right <b>[RemoveFromRight]</b>	Defines the number of digits to remove from the right of the telephone number prefix. For example, if you enter 3 and the phone number is 5551234, the new phone number is 5551.
Web: Prefix to Add EMS: Prefix/Suffix To Add CLI: prefix-to-add	Defines the number or string that you want added to the front of the telephone number. For example, if you enter 9 and the phone number is 1234, the new number is 91234.

Parameter	Description
<b>[Prefix2Add]</b>	
Web: Suffix to Add EMS: Prefix/Suffix To Add CLI: suffix-to-add <b>[Suffix2Add]</b>	Defines the number or string that you want added to the end of the telephone number. For example, if you enter 00 and the phone number is 1234, the new number is 123400.
Web/EMS: Number of Digits to Leave CLI: num-of-digits-to-leave <b>[LeaveFromRight]</b>	Defines the number of digits that you want to keep from the right of the phone number. For example, if you enter 4 and the phone number is 00165751234, then the new number is 1234.
Web: NPI EMS: Number Plan CLI: np <b>[NumberPlan]</b>	<p>Defines the Numbering Plan Indicator (NPI).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Unknown (default)</li> <li>▪ <b>[9]</b> Private</li> <li>▪ <b>[1]</b> E.164 Public</li> <li>▪ <b>[-1]</b> Not Configured = value received from PSTN/IP is used</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to number manipulation tables for IP-to-Tel calls.</li> <li>▪ NPI can be used in the SIP Remote-Party-ID header by using the EnableRPIHeader and AddTON2RPI parameters.</li> <li>▪ For more information on available NPI/TON values, see Numbering Plans and Type of Number on page 319.</li> </ul>
Web: TON EMS: Number Type CLI: ton <b>[NumberType]</b>	<p>Defines the Type of Number (TON).</p> <ul style="list-style-type: none"> <li>▪ If you selected 'Unknown' for the NPI, you can select Unknown <b>[0]</b>.</li> <li>▪ If you selected 'Private' for the NPI, you can select Unknown <b>[0]</b>, Level 2 Regional <b>[1]</b>, Level 1 Regional <b>[2]</b>, PISN Specific <b>[3]</b> or Level 0 Regional (Local) <b>[4]</b>.</li> <li>▪ If you selected 'E.164 Public' for the NPI, you can select Unknown <b>[0]</b>, International <b>[1]</b>, National <b>[2]</b>, Network Specific <b>[3]</b>, Subscriber <b>[4]</b> or Abbreviated <b>[6]</b>.</li> </ul> <p>The default is 'Unknown'.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to number manipulation tables for IP-to-Tel calls.</li> <li>▪ TON can be used in the SIP Remote-Party-ID header by using the EnableRPIHeader and AddTON2RPI parameters.</li> <li>▪ For more information on available NPI/TON values, see Numbering Plans and Type of Number on page 319.</li> </ul>
Web: Presentation EMS: Is Presentation Restricted CLI: is-presentation-restricted <b>[IsPresentationRestricted]</b>	<p>Enables caller ID.</p> <ul style="list-style-type: none"> <li>▪ Not Configured = Privacy is determined according to the Caller ID table (see Configuring Caller Display Information on page 398).</li> <li>▪ <b>[0]</b> Allowed = Sends Caller ID information when a call is made using these destination/source prefixes.</li> <li>▪ <b>[1]</b> Restricted = Restricts Caller ID information for these prefixes.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This field is applicable only to number manipulation tables for source phone number manipulation.</li> <li>▪ If this field is set to <b>Restricted</b> and the 'Asserted Identity Mode' (AssertedIdMode) parameter is set to <b>Add P-Asserted-Identity</b>,</li> </ul>

Parameter	Description
	the From header in the INVITE message includes the following: From: 'anonymous' <sip: anonymous@anonymous.invalid> and 'privacy: id' header.

## 27.3 Manipulating Number Prefix

The device supports a notation for adding a prefix where part of the prefix is first extracted from a user-defined location in the original destination or source number. This notation is entered in the 'Prefix to Add' field in the Number Manipulation tables (see 'Configuring Source/Destination Number Manipulation' on page 297):  $x[n,l]y...$

where,

- $x$  = any number of characters/digits to add at the beginning of the number (i.e. first digits in the prefix).
- $[n,l]$  = defines the location in the original destination or source number where the digits  $y$  are added:
  - $n$  = location (number of digits counted from the left of the number) of a specific string in the original destination or source number.
  - $l$  = number of digits that this string includes.
- $y$  = prefix to add at the specified location.

For example, assume that you want to manipulate an incoming IP call with destination number +5492028888888 (area code 202 and phone number 8888888) to the number 0202158888888. To perform such a manipulation, the following configuration is required in the Number Manipulation table:

1. The following notation is used in the 'Prefix to Add' field:  
 $0[5,3]15$   
where,
  - 0 is the number to add at the beginning of the original destination number.
  - $[5,3]$  denotes a string that is located after (and including) the fifth character (i.e., the first '2' in the example) of the original destination number, and its length being three digits (i.e., the area code 202, in the example).
  - 15 is the number to add immediately after the string denoted by  $[5,3]$  - in other words, 15 is added after (i.e. to the right of) the digits 202.
2. The first seven digits from the left are removed from the original number, by entering "7" in the 'Stripped Digits From Left' field.

### Example of Configured Rule for Manipulating Prefix using Special Notation

Parameter	Rule 1
Destination Prefix	+5492028888888
Source Prefix	*
Source IP Address	*
Stripped Digits from Left	7
Prefix to Add	$0[5,3]15$

In this configuration example, the following manipulation process occurs:

1. The prefix is calculated as 020215.
2. The first seven digits from the left are removed from the original number, thereby changing the number to 8888888.
3. The prefix that was previously calculated is then added.

## 27.4 SIP Calling Name Manipulations

The Calling Name Manipulations Tel2IP and Calling Name Manipulations IP2Tel tables allow you to configure up to 120 manipulation rules for manipulating the calling name (i.e., caller ID) in SIP messages. This can include modifying or removing the calling name. SIP calling name manipulation is applicable to Tel-to-IP and IP-to-Tel calls.

For example, assume that an incoming SIP INVITE message includes the following header:

```
P-Asserted-Identity: "company:john" sip:6666@78.97.79.104
```

Using the Calling Name Manipulations IP2Tel table, the text "company" can be changed to "worker" in the outgoing INVITE, as shown below:

```
P-Asserted-Identity: "worker:john" sip:996666@10.13.83.10
```

The calling name manipulation tables provide two configuration areas:

- Matching characteristics (*Rule*) of incoming call, for example, prefix of destination number.
- Manipulation operation (*Action*), for example, remove user-defined number of digits from the left of the calling name.

If the incoming call matches the characteristics of a rule, then its manipulation action is applied.



### Notes:

- For configuring the Calling Name Manipulation Table for Tel > IP Calls table for retrieving the calling name (display name) from an Active Directory using LDAP queries, see 'Querying the AD for Calling Name' on page 188.
- The Calling Name Manipulations Tel2IP table can also be configured using the table *ini* file parameter, CallingNameMapTel2Ip or CLI command, configure voip/gw manipulations calling-name-map-tel2ip.
- The Calling Name Manipulations IP2Tel table can also be configured using the table *ini* file parameter, CallingNameMapIp2Tel or CLI command, configure voip/gw manipulations calling-name-map-ip2tel.

➤ **To configure calling name manipulation rules:**

1. Open the required Calling Name Manipulations page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** > **Calling Name IP->Tel** or **Calling Name Tel->IP**).
2. Click the **Add** button; the following dialog box appears:

**Figure 27-3: Calling Name Manipulation IP2Tel - Rule Tab**

3. Click the **Rule** tab, and then configure the matching characteristics. For a description of the parameters, see the table below.
4. Click the **Action** tab, and then configure the manipulation operation. For a description of the parameters, see the table below.
5. Click the **Submit** button to save your changes.

**Calling Name Manipulation Parameters Description**

Parameter	Description
<b>Matching Characteristics (Rule)</b>	
Web: Destination Prefix CLI: dst-prefix	Defines the destination (called) telephone number prefix and/or suffix. You can use special notations for denoting the prefix. For example, <b>[100-199](100,101,105)</b> denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. You can also use the \$ sign to denote calls without a called number. For a description of available notations, see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 659.
Web/EMS: Source Prefix CLI: src-prefix	Defines the source (calling) telephone number prefix and/or suffix. You can use special notations for denoting the prefix. For example, <b>[100-199](100,101,105)</b> denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. You can also use the \$ sign to denote calls without a calling number. For a description of available notations, see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 659.
Web: Calling Name Prefix CLI: calling-name-prefix	Defines the caller name (i.e., caller ID) prefix. You can use special notations for denoting the prefix. For example, to denote any prefix, use the asterisk (*) symbol or to denote calls without a calling name, use the \$ sign. For a description of available notations, see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 659.

Parameter	Description
Web: Source Trunk Group ID CLI: src-trunk-group-id	Defines the source Trunk Group ID for Tel-to-IP calls. To denote all Trunk Groups, leave this field empty. <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Calling Name Manipulations Tel2IP table.</li> <li>The value -1 indicates that this field is ignored in the rule.</li> <li>This parameter is applicable only to Tel-to-IP calls.</li> </ul>
Web: Source IP Group ID CLI: src-ip-group-id	Defines the IP Group from where the IP call originated. <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Calling Name Manipulations Tel2IP table.</li> <li>The value -1 indicates that this field is ignored in the rule.</li> </ul>
Web/EMS: Source IP Address CLI: src-ip-address	Defines the source IP address of the caller, obtained from the Contact header in the INVITE message. <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Calling Name Manipulations IP2Tel table.</li> <li>The source IP address can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 to 10.8.8.99.</li> <li>The source IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all IP addresses between 10.8.8.0 and 10.8.8.255.</li> </ul>
Web: Source Host Prefix CLI: src-host-prefix	Defines the URI host name prefix of the incoming SIP INVITE message in the From header. <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Calling Name Manipulations IP2Tel table.</li> <li>The asterisk (*) wildcard can be used to denote any prefix.</li> <li>If the P-Asserted-Identity header is present in the incoming INVITE message, then the value of this parameter is compared to the P-Asserted-Identity URI host name (instead of the From header).</li> </ul>
Web: Destination Host Prefix CLI: dst-host-prefix	Defines the Request-URI host name prefix of the incoming SIP INVITE message. <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Calling Name Manipulations IP2Tel table.</li> <li>The asterisk (*) wildcard can be used to denote any prefix.</li> </ul>
<b>Operation (Action)</b>	
Web: Stripped Digits From Left EMS: Number Of Stripped Digits CLI: remove-from-left	Defines the number of characters to remove from the left of the calling name. For example, if you enter 3 and the calling name is "company:john", the new calling name is "pany:john".
Web: Stripped Digits From Right EMS: Number Of Stripped Digits CLI: remove-from-right	Defines the number of characters to remove from the right of the calling name. For example, if you enter 3 and the calling name is "company:name", the new name is "company:n".

Parameter	Description
Web/EMS: Number of Digits to Leave CLI: num-of-digits-to-leave	Defines the number of characters that you want to keep from the right of the calling name. For example, if you enter 4 and the calling name is "company:name", the new name is "name".
Web: Prefix to Add EMS: Prefix/Suffix To Add CLI: prefix-to-add	Defines the number or string to add at the front of the calling name. For example, if you enter ITSP and the calling name is "company:name", the new name is ITSPcompany:john".
Web: Suffix to Add EMS: Prefix/Suffix To Add CLI: suffix-to-add	Defines the number or string to add at the end of the calling name. For example, if you enter 00 and calling name is "company:name", the new name is "company:name00".

## 27.5 Configuring Redirect Number IP to Tel

You can configure rules for manipulating the redirect number received in the incoming message:

- IP-to-Tel redirect number manipulation: You can manipulate the value of the received SIP Diversion, Resource-Priority, or History-Info headers, which is then added to the Redirecting Number Information Element (IE) in the ISDN Setup message sent to the Tel side. This also includes the reason for the call redirection. This is configured in the Redirect Number IP > Tel table.
- Tel-to-IP redirect number manipulation: You can manipulate the prefix of the redirect number, received from the Tel side, in the outgoing SIP Diversion, Resource-Priority, or History-Info headers sent to the IP side. This is configured in the Redirect Number Tel > IP table.

The redirect number manipulation tables provide two configuration areas:

- Matching characteristics (*Rule*) of incoming call, for example, prefix of redirect number.
- Manipulation operation (*Action*), for example, remove user-defined number of digits from the left of the redirect number.

If the incoming call matches the characteristics of a rule, then its manipulation action is applied.



### Notes:

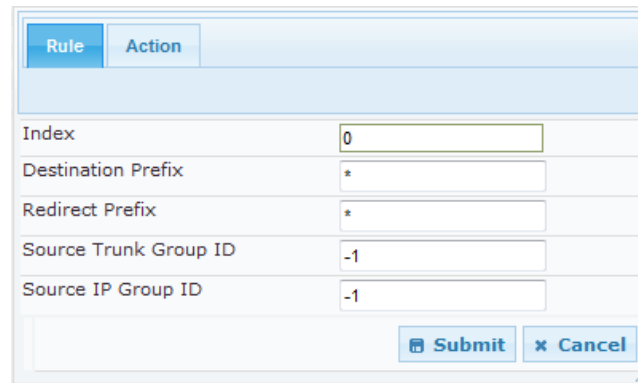
- If the device copies the received destination number to the outgoing SIP redirect number (enabled by the CopyDest2RedirectNumber parameter), then no redirect number Tel-to-IP manipulation is done.
- The manipulation rules are done in the following order: Stripped Digits From Left, Stripped Digits From Right, Number of Digits to Leave, Prefix to Add, and then Suffix to Add.
- The Redirect Prefix parameter is used before it is manipulated.
- The redirect number manipulation tables can also be configured using the ini file and CLI:
  - Redirect Number IP to Tel table: RedirectNumberMapIp2Tel (ini); configure voip/gw manipulations redirect-number-map-ip2tel (CLI)
  - Redirect Number Tel to IP table: RedirectNumberMapTel2Ip (ini); configure voip/gw manipulations redirect-number-map-tel2ip (CLI)



➤ **To configure redirect number manipulation rules:**

1. Open the required redirect number manipulation table (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** > **Redirect Number Tel > IP** or **Redirect Number IP > Tel**).
2. Click the **Add** button; the following dialog box appears (e.g., **Redirect Number Tel > IP** table):

**Figure 27-4: Redirect Number Manipulation (e.g., Tel to IP)**



3. Click the **Rule** tab, and then configure the matching characteristics. For a description of the parameters, see the table below.
4. Click the **Action** tab, and then configure the manipulation operation. For a description of the parameters, see the table below.
5. Click **Submit** to apply your settings.

**Redirect Number Manipulation Parameters Description**

Parameter	Description
<b>Matching Characteristics (Rule)</b>	
Web/EMS: Redirect Prefix CLI: redirect-prefix <b>[RedirectPrefix]</b>	Defines the redirect telephone number prefix. To denote any number, use the wildcard asterisk (*) symbol.
Web/EMS: Destination Prefix CLI: dst-prefix <b>[DestinationPrefix]</b>	Defines the destination (called) telephone number prefix. To denote any number, use the wildcard asterisk (*) symbol. For manipulating the diverting and redirected numbers for call diversion, you can use the strings "DN" and "RN" to denote the destination prefix of these numbers. For more information, see <a href="#">Manipulating Redirected and Diverted Numbers for Call Diversion</a> on page 310.
Web: Source Trunk Group ID CLI: src-trunk-group-id <b>[SrcTrunkGroupID]</b>	Defines the Trunk Group from where the Tel call is received. To denote any Trunk Group, leave this field empty. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to the Redirect Number Tel &gt; IP table.</li> <li>▪ The value -1 indicates that this field is ignored in the rule.</li> <li>▪ For IP-to-IP call routing, this parameter is not relevant.</li> </ul>
Source IP Group ID CLI: src-ip-group-id <b>[SrcIPGroupID]</b>	Defines the IP Group from where the IP call originated. Typically, the IP Group of an incoming INVITE is determined or classified by the Inbound IP Routing Table. If not used (i.e., any IP Group), leave the field empty. <b>Notes:</b>



Parameter	Description
	<ul style="list-style-type: none"> <li>This parameter is applicable only to the Redirect Number Tel &gt; IP table.</li> <li>This parameter is applicable only to the IP-to-IP application.</li> <li>The value -1 indicates that it is ignored in the rule.</li> </ul>
Web/EMS: Source IP Address CLI: src-ip-address <b>[SourceAddress]</b>	<p>Defines the IP address of the caller. This is obtained from the Contact header in the INVITE message.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Redirect Number IP &gt; Tel table.</li> <li>The source IP address can include the following wildcards: <ul style="list-style-type: none"> <li>✓ "x": represents single digits. For example, 10.8.8.xx denotes all addresses between 10.8.8.10 and 10.8.8.99.</li> <li>✓ "*": represents any number between 0 and 255. For example, 10.8.8.* denotes all addresses between 10.8.8.0 and 10.8.8.255.</li> </ul> </li> </ul>
Web: Source Host Prefix CLI: src-host-prefix <b>[SrcHost]</b>	<p>Defines the URI host name prefix of the incoming SIP INVITE message in the From header.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Redirect Number IP &gt; Tel table.</li> <li>Use the wildcard asterisk (*) symbol to denote any prefix.</li> <li>If the P-Asserted-Identity header is present in the incoming INVITE message, then the value of this parameter is compared to the P-Asserted-Identity URI host name (instead of to the From header).</li> </ul>
Web: Destination Host Prefix CLI: dst-host-prefix <b>[DestHost]</b>	<p>Defines the Request-URI host name prefix of the incoming SIP INVITE message.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Redirect Number IP &gt; Tel table.</li> <li>Use the wildcard asterisk (*) symbol to denote any prefix.</li> </ul>
<b>Operation (Action)</b>	
Web: Stripped Digits From Left EMS: Remove From Left CLI: remove-from-left <b>[RemoveFromLeft]</b>	<p>Defines the number of digits to remove from the left of the redirect number prefix. For example, if you enter 3 and the redirect number is 5551234, the new number is 1234.</p>
Web: Stripped Digits From Right EMS: Remove From Right CLI: remove-from-right <b>[RemoveFromRight]</b>	<p>Defines the number of digits to remove from the right of the redirect number prefix. For example, if you enter 3 and the redirect number is 5551234, the new number is 5551.</p>
Web/EMS: Number of Digits to Leave CLI: num-of-digits-to-leave <b>[LeaveFromRight]</b>	<p>Defines the number of digits that you want to retain from the right of the redirect number.</p>
Web/EMS: Prefix to Add CLI: prefix-to-add <b>[Prefix2Add]</b>	<p>Defines the number or string that you want added to the front of the redirect number. For example, if you enter 9 and the redirect number is 1234, the new number is 91234.</p>
Web/EMS: Suffix to Add	<p>Defines the number or string that you want added to the end of the</p>

Parameter	Description
CLI: suffix-to-add <b>[Suffix2Add]</b>	redirect number. For example, if you enter 00 and the redirect number is 1234, the new number is 123400.
Web: Presentation EMS: Is Presentation Restricted CLI: is-presentation-restricted <b>[IsPresentationRestricted]</b>	<p>Enables caller ID.</p> <ul style="list-style-type: none"> <li>Not Configured = Privacy is determined according to the Caller ID table (see Configuring Caller Display Information on page 398).</li> <li><b>[0]</b> Allowed = Sends Caller ID information when a call is made using these destination / source prefixes.</li> <li><b>[1]</b> Restricted = Restricts Caller ID information for these prefixes.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If 'Presentation' is set to 'Restricted' and the AssertedIdMode parameter is set to <b>Add P-Asserted-Identity</b>, the From header in the INVITE message includes the following: From: 'anonymous' &lt;sip: anonymous@anonymous.invalid&gt; and 'privacy: id' header.</li> </ul>
Web: TON EMS: Number Type CLI: ton <b>[NumberType]</b>	<p>Defines the Type of Number (TON). The default is 'Unknown' <b>[0]</b>.</p> <ul style="list-style-type: none"> <li>If you select 'Unknown' for the NPI, you can select Unknown <b>[0]</b>.</li> <li>If you select 'Private' for the NPI, you can select Unknown <b>[0]</b>, International <b>[1]</b>, National <b>[2]</b>, Network Specific <b>[3]</b> or Subscriber <b>[4]</b>.</li> <li>If you select 'E.164 Public' for the NPI, you can select Unknown <b>[0]</b>, International <b>[1]</b>, National <b>[2]</b>, Network Specific <b>[3]</b>, Subscriber <b>[4]</b> or Abbreviated <b>[6]</b>.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Redirect Number IP &gt; Tel table.</li> <li>For more information on available NPI/TON values, see Numbering Plans and Type of Number on page 319.</li> </ul>
Web: NPI EMS: Number Plan CLI: np <b>[NumberPlan]</b>	<p>Defines the Numbering Plan Indicator (NPI).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Unknown (default)</li> <li><b>[9]</b> Private</li> <li><b>[1]</b> E.164 Public</li> <li><b>[-1]</b> Not Configured = value received from PSTN/IP is used</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Redirect Number IP &gt; Tel table.</li> <li>For more information on available NPI/TON values, see Numbering Plans and Type of Number on page 319.</li> </ul>

## 27.6 Manipulating Redirected and Diverted Numbers for Call Diversion

You can configure manipulation rules to manipulate the Diverted-to and Diverting numbers received in the incoming Call Redirection Facility message for call diversion, which is interworked to outgoing SIP 302 responses. This feature is applicable to the Euro ISDN and QSIG variants, and to IP-to-Tel calls.

The incoming redirection Facility message includes, among other parameters, the Diverted-to number and Diverting number. The Diverted-to number (i.e., new destination) is mapped to the user part in the Contact header of the SIP 302 response. The Diverting number is mapped to the user part in the Diversion header of the SIP 302 response.

These two numbers can be manipulated by entering the following special strings in the 'Destination Prefix' field of the Redirect Number Tel -> IP manipulation table:

- "RN" - used in the rule to manipulate the Redirected number (i.e., originally called number or Diverting number).
- "DN" - used in the rule to manipulate the Diverted-to number (i.e., the new called number or destination). This manipulation is done on the user part in the Contact header of the SIP 302 response.

For example, assume the following required manipulation:

- Manipulate Redirected number 6001 (originally called number) to 6005
- Manipulate Diverted-to number 8002 (the new called number or destination) to 8005

The configuration in the Redirect Number Tel -> IP manipulation table is as follows:

**Redirect Number Configuration Example**

Parameter	Rule 1	Rule 2
Destination Prefix	RN	DN
Redirect Prefix	6	8
Stripped Digits From Right	1	1
Suffix to Add	5	5
Number of Digits to Leave	5	-

After the above manipulation is done, the device sends the following outgoing SIP 302 response:

```
SIP/2.0 302 Moved Temporarily
Via: SIP/2.0/TLS 10.33.45.68;branch=z9hG4bKac54132643;alias
From: "MP118 1" <sip:8001@10.33.45.68>;tag=1c54119560
To: <sip:6001@10.33.45.69;user=phone>;tag=1c664560944
Call-ID: 541189832710201115142@10.33.45.68
CSeq: 1 INVITE
Contact: <sip:8005@10.33.45.68;user=phone>
Supported: em,timer,replaces,path,early-session,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE,UPDATE
Diversion: <tel:6005>;reason=unknown;counter=1
Server: Audiocodes-Sip-Gateway-IPmedia 260_UN/v.6.20A.043.001
Reason: SIP ;cause=302 ;text="302 Moved Temporarily"
Content-Length: 0
```

## 27.7 Mapping NPI/TON to SIP Phone-Context

The Phone-Context table page allows you to map Numbering Plan Indication (NPI) and Type of Number (TON) to the SIP 'phone-context' parameter. The 'phone-context' parameter appears in the standard SIP headers where a phone number is used (i.e., Request-URI, To, From, and Diversion). When a call is received from the ISDN/Tel side, the NPI and TON are compared against the table and the matching 'phone-context' value is used in the outgoing SIP INVITE message. The same mapping occurs when an INVITE with a 'phone-context' parameter is received.

For example, for a Tel-to-IP call with NPI/TON set as E164 National (values 1/2), the device sends the following SIP INVITE URI:

```
sip:12365432;phone-context= na.e.164.nt.com
```

This is configured for entry 3 in the figure below. In the opposite direction (IP-to-Tel call), if the incoming INVITE contains this 'phone-context' (e.g. "phone-context= na.e.164.nt.com"), the NPI/TON of the called number in the outgoing Setup message is changed to E164 National.

➤ **To configure NPI/TON to SIP phone-context rules:**

1. Open the Phone Context Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** > **Phone Context**).

**Figure 27-5: Phone Context Table Page**

Add Phone Context As Prefix		Enable
Phone Context Index		1-10

	NPI	TON	Phone Context
1	Unknown	Unknown	unknown.com
2	Private	Level 2 Regional	host.com
3	E.164 Public	National	na.e164.host.com
4			

2. Configure the parameters as required. For a description of the parameters, see the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.



**Notes:**

- You can configure multiple rows with the same NPI/TON or same SIP 'phone-context'. In such a configuration, a Tel-to-IP call uses the first matching rule in the table.
- The Phone Context table can also be configured using the table ini file parameter, PhoneContext (see 'Number Manipulation Parameters' on page 859) or CLI command, configure voip > gw manipulations phone-context-table.

**Phone-Context Parameters Description**

Parameter	Description
Add Phone Context As Prefix CLI: configure voip > gw manipulations general-setting > add-ph-cntxt-as-pref <b>[AddPhoneContextAsPrefix]</b>	Determines whether the received SIP 'phone-context' parameter is added as a prefix to the outgoing ISDN Setup message (for digital interfaces) with called and calling numbers. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
NPI CLI: np	Defines the Number Plan Indicator (NPI).

Parameter	Description
[PhoneContext_Npi]	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> Unknown (default)</li> <li>▪ <b>[1]</b> E.164 Public</li> <li>▪ <b>[9]</b> Private</li> </ul> <p>For a detailed list of the available NPI/TON values, see Numbering Plans and Type of Number on page 319.</p>
TON CLI: ton [PhoneContext_Ton]	<p>Defines the Type of Number (TON).</p> <ul style="list-style-type: none"> <li>▪ If you selected Unknown as the NPI, you can select Unknown <b>[0]</b>.</li> <li>▪ If you selected Private as the NPI, you can select one of the following: <ul style="list-style-type: none"> <li>✓ <b>[0]</b> Unknown</li> <li>✓ <b>[1]</b> Level 2 Regional</li> <li>✓ <b>[2]</b> Level 1 Regional</li> <li>✓ <b>[3]</b> PSTN Specific</li> <li>✓ <b>[4]</b> Level 0 Regional (Local)</li> </ul> </li> <li>▪ If you selected E.164 Public as the NPI, you can select one of the following: <ul style="list-style-type: none"> <li>✓ <b>[0]</b> Unknown</li> <li>✓ <b>[1]</b> International</li> <li>✓ <b>[2]</b> National</li> <li>✓ <b>[3]</b> Network Specific</li> <li>✓ <b>[4]</b> Subscriber</li> <li>✓ <b>[6]</b> Abbreviated</li> </ul> </li> </ul>
Phone Context CLI: context [PhoneContext_Context]	Defines the SIP 'phone-context' URI parameter.

## 27.8 Configuring Release Cause Mapping

The Release Cause Mapping table allows you to map up to 12 different ISDN ITU-T Q.850 cause codes, which indicate reasons for ISDN call failure, to SIP response codes, and vice versa. This allows you to override the default release cause mappings between ISDN and SIP, as described in 'Fixed Mapping of ISDN Release Reason to SIP Response' on page 316 and 'Fixed Mapping of SIP Response to ISDN Release Reason' on page 314.



### Notes:

- For Tel-to-IP calls, you can also map the less commonly used SIP responses to a single default ISDN Release Cause, using the DefaultCauseMapISDN2IP parameter. This parameter defines a default ISDN Cause that is always used except when the following Release Causes are received: Normal Call Clearing (16), User Busy (17), No User Responding (18) or No Answer from User (19).
- The release cause mapping tables can also be configured using the ini file and CLI:
  - 1) Release Cause Mapping from ISDN to SIP table:  
CauseMapISDN2SIP (ini) or CLI command, configure voip > gw manipulations cause-map-isdn2sip.
  - 2) Release Cause Mapping from SIP to ISDN  
table:CauseMapSIP2ISDN (ini) or CLI command, configure voip > gw manipulations cause-map-sip2isdn.

➤ **To configure Release Cause mapping:**

1. Open the Release Cause Mapping page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** > **Release Cause Mapping**).

**Figure 27-6: Release Cause Mapping Page**

Release Cause Mapping from ISDN to SIP			
	Q.850 Cause		SIP Response
1	<input type="text"/>		<input type="text"/>
2	<input type="text"/>		<input type="text"/>
3	<input type="text"/>		<input type="text"/>
4	<input type="text"/>		<input type="text"/>
5	<input type="text"/>		<input type="text"/>
6	<input type="text"/>		<input type="text"/>
7	<input type="text"/>		<input type="text"/>
8	<input type="text"/>		<input type="text"/>
9	<input type="text"/>		<input type="text"/>
10	<input type="text"/>		<input type="text"/>
11	<input type="text"/>		<input type="text"/>
12	<input type="text"/>		<input type="text"/>

Release Cause Mapping from SIP to ISDN			
	SIP Response		Q.850 Cause
1	<input type="text"/>		<input type="text"/>
2	<input type="text"/>		<input type="text"/>
3	<input type="text"/>		<input type="text"/>

2. In the 'Release Cause Mapping from ISDN to SIP' group, map different Q.850 Release Causes to SIP Responses.
3. In the 'Release Cause Mapping from SIP to ISDN' group, map different SIP Responses to Q.850 Release Causes.
4. Click **Submit** to apply your changes.

## 27.8.1 Fixed Mapping of SIP Response to ISDN Release Reason

The following table describes the mapping of SIP response to ISDN release reason.

**Mapping of SIP Response to ISDN Release Reason**

SIP Response	Description	ISDN Release Reason	Description
400*	Bad request	31	Normal, unspecified
401	Unauthorized	21	Call rejected
402	Payment required	21	Call rejected
403	Forbidden	21	Call rejected
404	Not found	1	Unallocated number
405	Method not allowed	63	Service/option unavailable
406	Not acceptable	79	Service/option not implemented
407	Proxy authentication	21	Call rejected

SIP Response	Description	ISDN Release Reason	Description
	required		
408	Request timeout	102	Recovery on timer expiry
409	Conflict	41	Temporary failure
410	Gone	22	Number changed w/o diagnostic
411	Length required	127	Interworking
413	Request entity too long	127	Interworking
414	Request URI too long	127	Interworking
415	Unsupported media type	79	Service/option not implemented
420	Bad extension	127	Interworking
480	Temporarily unavailable	18	No user responding
481*	Call leg/transaction doesn't exist	127	Interworking
482*	Loop detected	127	Interworking
483	Too many hops	127	Interworking
484	Address incomplete	28	Invalid number format
485	Ambiguous	1	Unallocated number
486	Busy here	17	User busy
488	Not acceptable here	31	Normal, unspecified
500	Server internal error	41	Temporary failure
501	Not implemented	38	Network out of order
502	Bad gateway	38	Network out of order
503	Service unavailable	41	Temporary failure
504	Server timeout	102	Recovery on timer expiry
505*	Version not supported	127	Interworking
600	Busy everywhere	17	User busy
603	Decline	21	Call rejected
604	Does not exist anywhere	1	Unallocated number
606*	Not acceptable	38	Network out of order

\* Messages and responses were created because the 'ISUP to SIP Mapping' draft does not specify their cause code mapping.

## 27.8.2 Fixed Mapping of ISDN Release Reason to SIP Response

The following table describes the mapping of ISDN release reason to SIP response.

**Mapping of ISDN Release Reason to SIP Response**

ISDN Release Reason	Description	SIP Response	Description
1	Unallocated number	404	Not found
2	No route to network	404	Not found
3	No route to destination	404	Not found
6	Channel unacceptable	406*	Not acceptable
7	Call awarded and being delivered in an established channel	500	Server internal error
16	Normal call clearing	- *	BYE
17	User busy	486	Busy here
18	No user responding	408	Request timeout
19	No answer from the user	480	Temporarily unavailable
21	Call rejected	403	Forbidden
22	Number changed w/o diagnostic	410	Gone
26	Non-selected user clearing	404	Not found
27	Destination out of order	502	Bad gateway
28	Address incomplete	484	Address incomplete
29	Facility rejected	501	Not implemented
30	Response to status enquiry	501*	Not implemented
31	Normal unspecified	480	Temporarily unavailable
34	No circuit available	503	Service unavailable
38	Network out of order	503	Service unavailable
41	Temporary failure	503	Service unavailable
42	Switching equipment congestion	503	Service unavailable
43	Access information discarded	502*	Bad gateway
44	Requested channel not available	503*	Service unavailable
47	Resource unavailable	503	Service unavailable
49	QoS unavailable	503*	Service unavailable
50	Facility not subscribed	503*	Service unavailable
55	Incoming calls barred within CUG	403	Forbidden
57	Bearer capability not authorized	403	Forbidden
58	Bearer capability not presently available	503	Service unavailable
63	Service/option not available	503*	Service unavailable



ISDN Release Reason	Description	SIP Response	Description
65	Bearer capability not implemented	501	Not implemented
66	Channel type not implemented	480*	Temporarily unavailable
69	Requested facility not implemented	503*	Service unavailable
70	Only restricted digital information bearer capability is available	503*	Service unavailable
79	Service or option not implemented	501	Not implemented
81	Invalid call reference value	502*	Bad gateway
82	Identified channel does not exist	502*	Bad gateway
83	Suspended call exists, but this call identity does not	503*	Service unavailable
84	Call identity in use	503*	Service unavailable
85	No call suspended	503*	Service unavailable
86	Call having the requested call identity has been cleared	408*	Request timeout
87	User not member of CUG	503	Service unavailable
88	Incompatible destination	503	Service unavailable
91	Invalid transit network selection	502*	Bad gateway
95	Invalid message	503	Service unavailable
96	Mandatory information element is missing	409*	Conflict
97	Message type non-existent or not implemented	480*	Temporarily not available
98	Message not compatible with call state or message type non-existent or not implemented	409*	Conflict
99	Information element non-existent or not implemented	480*	Not found
100	Invalid information elements contents	501*	Not implemented
101	Message not compatible with call state	503*	Service unavailable
102	Recovery of timer expiry	408	Request timeout
111	Protocol error	500	Server internal error
127	Interworking unspecified	500	Server internal error

\* Messages and responses were created because the 'ISUP to SIP Mapping' draft doesn't specify their cause code mapping.

### 27.8.3 Reason Header

The device supports the SIP Reason header according to RFC 3326. The Reason header conveys information describing the disconnection cause of a call:

- **Sending Reason header:** If a call is disconnected from the Tel side (ISDN), the Reason header is set to the received Q.850 cause in the appropriate message (BYE/CANCEL/final failure response) and sent to the SIP side. If the call is disconnected because of a SIP reason, the Reason header is set to the appropriate SIP response.
- **Receiving Reason header:** If a call is disconnected from the IP side and the SIP message includes the Reason header, it is sent to the Tel side according to the following logic:
  - If the Reason header includes a Q.850 cause, it is sent as is.
  - If the Reason header includes a SIP response:
    - ◆ If the message is a final response, the response status code is translated to Q.850 format and passed to ISDN.
    - ◆ If the message isn't a final response, it is translated to a Q.850 cause.
  - When the Reason header is received twice (i.e., SIP Reason and Q.850), the Q.850 takes precedence over the SIP reason and is sent to the Tel side.

### 27.8.4 Mapping PSTN Release Cause to SIP Response

The device's FXO interface interoperates between the SIP network and the PSTN/PBX. This interoperability includes the mapping of PSTN/PBX Call Progress tones to SIP 4xx or 5xx responses for IP-to-Tel calls. The converse is also true - for Tel-to-IP calls, the SIP 4xx or 5xx responses are mapped to tones played to the PSTN/PBX.

When establishing an IP-to-Tel call, the following rules are applied:

- If the remote party (PSTN/PBX) is busy and the FXO device detects a busy tone, it sends a SIP 486 Busy response to IP. If it detects a reorder tone, it sends a SIP 404 Not Found (no route to destination) to IP. In both cases the call is released. Note that if the 'Disconnect Call on Busy Tone Detection' parameter is set to **Disable**, the FXO device ignores the detection of busy and reorder tones and does not release the call.
- For all other FXS/FXO release types such as:
  - no free channels in the Trunk Group,
  - an appropriate call routing rule to a Trunk Group doesn't exist, or
  - the phone number isn't found

then the device sends a SIP response to the IP according to the 'Default Release Cause' parameter. This parameter defines Q.931 release causes. Its default value is **3**, which is mapped to the SIP 404 response. By changing its value to **34**, the SIP 503 response is sent. Other causes can be used as well.

## 27.9 Numbering Plans and Type of Number

The IP-to-Tel destination or source number manipulation tables allow you to classify numbers by their Numbering Plan Indication (NPI) and Type of Number (TON). The device supports all NPI/TON classifications used in the ETSI ISDN variant, as shown in the table below:

**NPI/TON Values for ETSI ISDN Variant**

NPI	TON	Description
Unknown [0]	Unknown [0]	A valid classification, but one that has no information about the numbering plan.
E.164 Public [1]	Unknown [0]	A public number in E.164 format, but no information on what kind of E.164 number.
	International [1]	A public number in complete international E.164 format, e.g., 16135551234.
	National [2]	A public number in complete national E.164 format, e.g., 6135551234.
	Network Specific [3]	The type of number "network specific number" is used to indicate administration / service number specific to the serving network, e.g., used to access an operator.
	Subscriber [4]	A public number in complete E.164 format representing a local subscriber, e.g., 5551234.
	Abbreviated [6]	The support of this code is network dependent. The number provided in this information element presents a shorthand representation of the complete number in the specified numbering plan as supported by the network.
Private [9]	Unknown [0]	A private number, but with no further information about the numbering plan.
	Level 2 Regional [1]	
	Level 1 Regional [2]	A private number with a location, e.g., 3932200.
	PISN Specific [3]	
	Level 0 Regional (local) [4]	A private local extension number, e.g., 2200.

For NI-2 and DMS-100 ISDN variants, the valid combinations of TON and NPI for calling and called numbers include (Plan/Type):

- 0/0 - Unknown/Unknown
- 1/1 - International number in ISDN/Telephony numbering plan
- 1/2 - National number in ISDN/Telephony numbering plan
- 1/4 - Subscriber (local) number in ISDN/Telephony numbering plan
- 9/4 - Subscriber (local) number in Private numbering plan

## 28 Routing

This section describes the configuration of call routing rules.

### 28.1 Configuring General Routing Parameters

The Routing General Parameters page allows you to configure general routing parameters. For a description of these parameters, see 'Configuration Parameters Reference' on page 661.

➤ **To configure general routing parameters:**

1. Open the Routing General Parameters page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** submenu > **General Parameters**).

General Parameters	
Add Hunt Group ID as Prefix	No
Add Trunk ID as Prefix	No
Replace Empty Destination with B-channel Phone Number	No
Add NPI and TON to Called Number	No
Add NPI and TON to Calling Number	No
IP to Tel Remove Routing Table Prefix	No
Source IP Address Input	SIP Contact Header
Enable Alt Routing Tel to IP	Disable
Alt Routing Tel to IP Mode	Both
Alt Routing Tel to IP Connectivity Method	ICMP Ping
Alt Routing Tel to IP Keep Alive Time	60
Alternative Routing Tone Duration [ms]	0
Source Manipulation Mode	FROM & PAI (after manipulation)
Max Allowed Packet Loss for Alt Routing [%]	20
Max Allowed Delay for Alt Routing [msec]	250

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.

### 28.2 Configuring Outbound IP Routing Table

The Outbound IP Routing Table page allows you to configure up to 180 Tel-to-IP or outbound IP call routing rules. The device uses these rules to route calls from the Tel or IP to a user-defined IP destination.

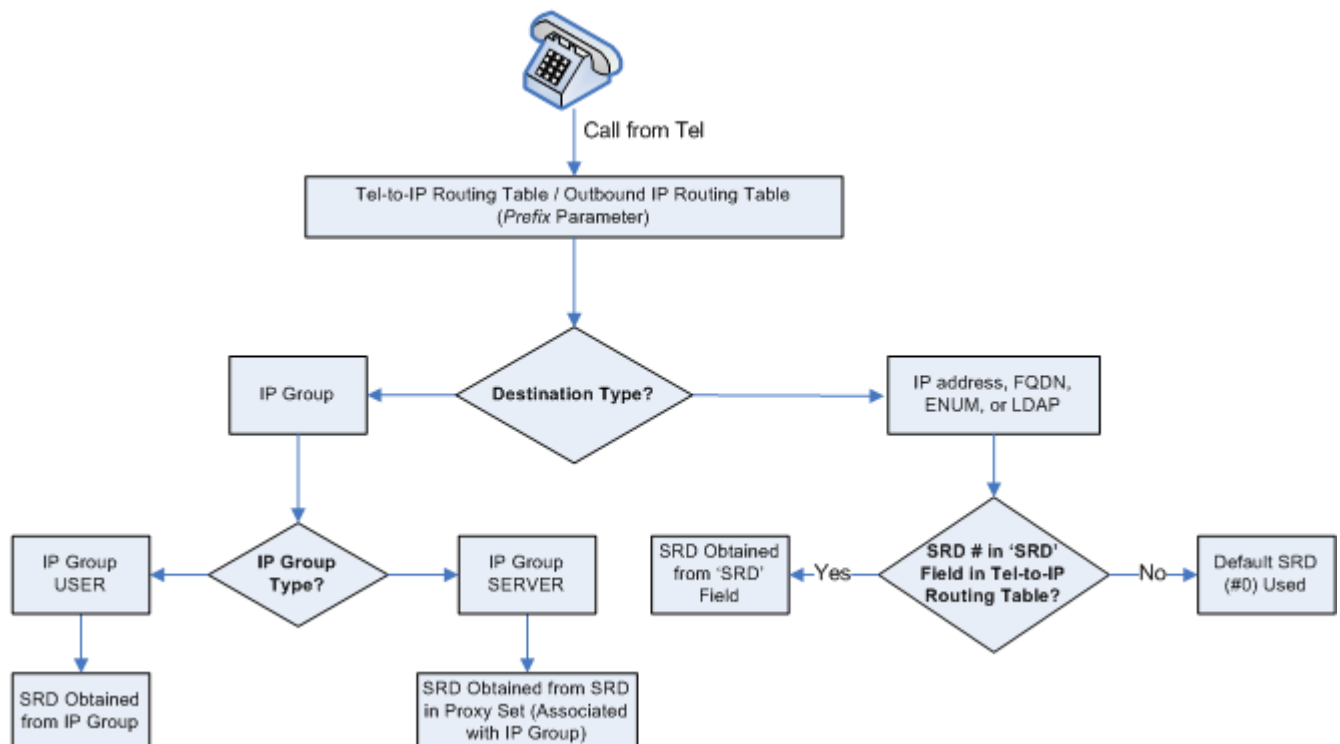
The Outbound IP Routing Table table provides two configuration areas:

- **Matching Characteristics:** Characteristics of the incoming call. If the call characteristics match a table entry, the routing rule is used to route the call to the specified destination. One or more characteristics can be defined for the rule:
  - Source IP Group (to which the call belongs)
  - Source and destination Request-URI host name prefix
  - Source Trunk Group (from where the call is received)
  - Source (calling) and destination (called) telephone number prefix and suffix
  - Source and destination Request-URI host name prefix

- **Destination:** If the call matches the configured characteristics, the device routes the call to an IP destination. If no characteristics match is found in the table, the call is rejected. The destination can be any of the following:
  - IP address in dotted-decimal notation.
  - Fully Qualified Domain Name (FQDN).
  - E.164 Telephone Number Mapping (ENUM service).
  - Lightweight Directory Access Protocol (LDAP). For a description, see 'Routing Based on LDAP Active Directory Queries' on page 179.
  - IP Group, where the call is routed to the IP address configured for the Proxy Set or SRD associated with the IP Group (configured in 'Configuring IP Groups' on page 204). If the device is configured with multiple SRDs, you can also indicate (in the table's 'Dest. SRD' field) the destination SRD for routing to one of the following destination types - IP address, FQDN, ENUM, or LDAP. If the SRD is not specified, then the default SRD (0) is used. In scenarios where routing is to an IP Group, the destination SRD is obtained from the SRD associated with the IP Group (in the IP Group table). The specified destination SRD determines the:
    - ◆ Destination SIP interface (SIP port and control IP interface) - important when using multiple SIP control VLANs
    - ◆ Media Realm (port and IP interface for media / RTP voice)
    - ◆ Other SRD-related interfaces and features on which the call is routed

Since each call must have a destination IP Group (even in cases where the destination type is not to an IP Group), in cases when the IP Group is not specified, the SRD's default IP Group is used, which is the first configured IP Group that belongs to the SRD.

**Figure 28-1: Locating SRD**





**Notes:** When using a proxy server, you do not need to configure this table, unless you require one of the following:

- Fallback (alternative) routing if communication is lost with the proxy server.
- IP security, whereby the device routes only received calls whose source IP addresses are defined in this table. IP security is enabled using the SecureCallsFromIP parameter.
- Filter Calls to IP feature: the device checks this table before a call is routed to the proxy server. However, if the number is not allowed, i.e., the number does not exist in the table or a Call Restriction (see below) routing rule is applied, the call is released.
- Obtain different SIP URI host names (per called number).
- Assign IP Profiles to calls.
- For this table to take precedence over a proxy for routing calls, you need to set the parameter PreferRouteTable to 1. The device checks the 'Destination IP Address' field in this table for a match with the outgoing call; a proxy is used only if a match is not found.

In addition to basic outbound IP routing, this table supports the following features:

- **Least Cost Routing (LCR):** If the LCR feature is enabled, the device searches the routing table for matching routing rules and then selects the one with the lowest call cost. The call cost of the routing rule is done by assigning it a Cost Group. For configuring Cost Groups, see 'Least Cost Routing' on page 189. If two routing rules have identical costs, then the rule appearing higher up in the table (i.e., first-matched rule) is used. If a selected route is unavailable, the device uses the next least-cost routing rule. However, even if a matched rule is not assigned a Cost Group, the device can select it as the preferred route over other matched routing rules with Cost Groups, according to the settings of the LCR parameter, LCRDefaultCost (see 'Enabling LCR and Configuring Default LCR' on page 191).
- **Call Forking:** If the Tel-to-IP Call Forking feature is enabled, the device can send a Tel call to multiple IP destinations. An incoming Tel call with multiple matched routing rules (e.g., all with the same source prefix numbers) can be sent (forked) to multiple IP destinations if the rules are defined with a Forking Group in the table. The call is established with the first IP destination that answers the call.
- **Call Restriction:** Rejects calls whose matching routing rule is configured with the destination IP address of 0.0.0.0.
- **Always Use Routing Table:** Even if a proxy server is used, the SIP Request-URI host name in the outgoing INVITE message is obtained from this table. Using this feature, you can assign a different SIP URI host name for different called and/or calling numbers. This feature is enabled using the AlwaysUseRouteTable parameter.
- **IP Profiles:** IP Profiles can be assigned to destination addresses (also when a proxy is used).
- **Alternative Routing (when a proxy isn't used):** An alternative IP destination can be configured for a specific call. To associate an alternative IP address to a called telephone number prefix, assign it with an additional entry with a different IP address, or use an FQDN that resolves into two IP addresses. For more information on alternative routing, see 'Alternative Routing for Tel-to-IP Calls' on page 335.


**Notes:**

- Outbound IP routing can be performed before or after number manipulation. This is configured using the RouteModeTel2IP parameter, as described below.
- The Outbound IP Routing Table can also be configured using the table *ini* file parameter, Prefix or CLI command, configure voip > gw routing tel2ip-routing.

➤ **To configure Tel-to-IP or outbound IP routing rules:**

1. Open the Outbound IP Routing Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing > Tel to IP Routing**).

**Figure 28-2: Outbound IP Routing Page**

	Src. IP Group ID	Src. Host Prefix	Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address
1	-1							
2	-1							
3	-1							
4	-1							
5	-1							

2. From the 'Routing Index' drop-down list, select the range of entries that you want to add.
3. Configure the routing rule as required. For a description of the parameters, see the table below.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 532.

The table below shows configuration examples of Tel-to-IP or outbound IP routing rules, where:

- **Rule 1 and Rule 2 (Least Cost Routing rule):** For both rules, the called (destination) phone number prefix is 10, the caller's (source) phone number prefix is 100, and the call is assigned IP Profile ID 1. However, Rule 1 is assigned a cheaper Cost Group than Rule 2, and therefore, the call is sent to the destination IP address (10.33.45.63) associated with Rule 1.
- **Rule 3 (IP Group destination rule):** For all callers (\*), if the called phone number prefix is 20, the call is sent to IP Group 1 (whose destination is the IP address configured for its associated Proxy Set ID).
- **Rule 4 (domain name destination rule):** If the called phone number prefix is 5, 7, 8, or 9 and the caller belongs to Trunk Group ID 1, the call is sent to domain.com.
- **Rule 5 (block rule):** For all callers (\*), if the called phone number prefix is 00, the call is rejected (discarded).
- **Rule 6 (IP-to-IP rule):** If an incoming IP call from Source IP Group 2 with domain.com as source host prefix in its SIP Request-URI, the IP call is sent to IP address 10.33.45.65.
- **Rule 7, Rule 8, and Rule 9 (Forking Group rule):** For all callers (\*), if the called phone number prefix is 100, the call is sent to Rule 7 and 9 (belonging to Forking Group "1"). If their destinations are unavailable and alternative routing is enabled, the call is sent to Rule 8 (Forking Group "2").



**Example of Tel-to-IP Source Phone Number Manipulation Rules**

Parameter	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7	Rule 8	Rule 9
Src. IP Group ID	-	-	-	-	-	2	-	-	-
Src. Trunk Group ID	*	0	1	-	-	-	-	-	-
Src. Host Prefix	-	-	-	-	-	domain.com	-	-	-
Src. Trunk Group ID	-	-	*	1	-	-	*	*	*
Dest. Phone Prefix	10	10	20	[5,7-9]	00	*	100	100	100
Source Phone Prefix	100	100	*	*	*	*	*	*	*
Dest. IP Address	10.33.45.63	10.33.45.50	-	domain.com	0.0.0.0	10.33.45.65	10.33.45.68	10.33.45.67	domain.com
Dest IP Group ID	-	-	1	-	-	-	-	-	-
IP Profile ID	1	1	-	-	-	-	-	-	-
Cost Group ID	Week end	Weekend_B	-	-	-	-	-	-	-
Forking Group			-	-	-	-	1	2	1

**Tel-to-IP / Outbound IP Routing Table Parameters**

Parameter	Description
<b>Matching Call Characteristics</b>	
Web/EMS: Tel to IP Routing Mode CLI: configure voip > gw routing general-setting > tel2ip-rte-mode <b>[RouteModeTel2IP]</b>	<p>Determines whether to route received calls to an IP destination before or after manipulation of the destination number.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Route calls before manipulation = Calls are routed before the number manipulation rules are applied (default).</li> <li><b>[1]</b> Route calls after manipulation = Calls are routed after the number manipulation rules are applied.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is not applicable if outbound proxy routing is used.</li> <li>For number manipulation, see 'Configuring Source/Destination Number Manipulation' on page 297.</li> </ul>

Parameter	Description
Web: Src. IP Group ID EMS: Source IP Group ID CLI: src-ip-group-id <b>[PREFIX_SrcIPGroupID]</b>	<p>Defines the IP Group from where the incoming IP call is received. Typically, the IP Group of an incoming INVITE is determined according to the Inbound IP Routing Table.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the IP-to-IP routing application.</li> <li>To denote all IP Groups, leave this field empty.</li> <li>If this IP Group has a Serving IP Group, then all calls from this IP Group are sent to the Serving IP Group. In such a scenario, this routing table is used only if the parameter PreferRouteTable is set to 1.</li> </ul>
Web: Src. Host Prefix EMS: Source Host Prefix CLI: src-host-prefix <b>[PREFIX_SrcHostPrefix]</b>	<p>Defines the prefix of the SIP Request-URI host name in the From header of the incoming SIP INVITE message.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To denote any prefix, use the asterisk (*) symbol.</li> <li>This parameter is applicable only to the IP-to-IP routing application.</li> </ul>
Web: Dest. Host Prefix EMS: Destination Host Prefix CLI: dst-host-prefix <b>[PREFIX_DestHostPrefix]</b>	<p>Defines the SIP Request-URI host name prefix of the incoming SIP INVITE message.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To denote any prefix, use the asterisk (*) symbol.</li> <li>This parameter is applicable only for IP-to-IP routing application.</li> </ul>
Web: Src. Trunk Group ID EMS: Source Trunk Group ID CLI: src-trunk-group-id <b>[PREFIX_SrcTrunkGroupID]</b>	<p>Defines the Trunk Group from where the call is received.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To denote any Trunk Group, use the asterisk (*) symbol.</li> <li>This parameter is applicable only to the Gateway application.</li> </ul>
Web: Dest. Phone Prefix EMS: Destination Phone Prefix CLI: dst-phone-prefix <b>[PREFIX_DestinationPrefix]</b>	<p>Defines the prefix and/or suffix of the called (destination) telephone number. The suffix is enclosed in parenthesis after the suffix value. You can use special notations for denoting the prefix. For example, <b>[100-199](100,101,105)</b> denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. To denote any prefix, use the asterisk (*) symbol or to denote calls without a called number, use the \$ sign. For a description of available notations, see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 659.</p> <p>The number can include up to 50 digits.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For LDAP-based routing, enter the LDAP query keyword as the prefix number to denote the IP domain: <ul style="list-style-type: none"> <li>✓ "PRIVATE" = Private number</li> <li>✓ "OCS" = Lync / OCS client number</li> <li>✓ "PBX" = PBX / IP PBX number</li> <li>✓ "MOBILE" = Mobile number</li> <li>✓ "LDAP_ERR" = LDAP query failure</li> </ul> For more information, see Routing Based on LDAP Active Directory Queries on page 179.</li> <li>If you want to configure re-routing of ISDN Tel-to-IP calls to fax destinations, you need to enter the value string "FAX" (case-sensitive) as</li> </ul>

Parameter	Description
	the destination phone prefix. For more information regarding this feature, see the FaxReroutingMode parameter.
Web/EMS: Source Phone Prefix CLI: src-phone-prefix <b>[PREFIX_SourcePrefix]</b>	<p>Defines the prefix and/or suffix of the calling (source) telephone number. You can use special notations for denoting the prefix. For example, <b>[100-199]</b>(100,101,105) denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. To denote any prefix, use the asterisk (*) symbol or to denote calls without a calling number, use the \$ sign. For a description of available notations, see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 659.</p> <p>The number can include up to 50 digits.</p>
<b>Operation (IP Destination)</b>	
Web: Dest. IP Address EMS: Address CLI: dst-ip-address <b>[PREFIX_DestAddress]</b>	<p>Defines the IP address (in dotted-decimal notation or FQDN) to where the call is sent. If an FQDN is used (e.g., domain.com), DNS resolution is done according to the DNSQueryType parameter.</p> <p>For ENUM-based routing, enter the string value "ENUM". The device sends an ENUM query containing the destination phone number to an external DNS server, configured in the Multiple Interface table. The ENUM reply includes a SIP URI which is used as the Request-URI in the subsequent outgoing INVITE and for routing (if a proxy is not used). To configure the type of ENUM service (e.g., e164.arpa), use the EnumService parameter.</p> <p>For LDAP-based routing, enter the string value "LDAP" for denoting the IP address of the LDAP server. For more information, see Routing Based on LDAP Active Directory Queries on page 179.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This field and any value assigned to it is ignored if you have configured a destination IP Group for this routing rule (in the 'Dest IP Group ID' field).</li> <li>▪ To reject calls, enter the IP address 0.0.0.0. For example, if you want to prohibit international calls, then in the 'Dest Phone Prefix' field, enter 00 and in the 'Dest IP Address' field, enter 0.0.0.0.</li> <li>▪ For routing calls between phones connected to the device (i.e., local routing), enter the device's IP address.</li> <li>▪ When the device's IP address is unknown (e.g., when DHCP is used), enter IP address 127.0.0.1.</li> <li>▪ When using domain names, enter the DNS server's IP address or alternatively, configure these names in the Internal DNS table (see 'Configuring the Internal DNS Table' on page 120).</li> <li>▪ The IP address can include the following wildcards: <ul style="list-style-type: none"> <li>✓ "x": represents single digits. For example, 10.8.8.xx denotes all addresses between 10.8.8.10 and 10.8.8.99.</li> <li>✓ "**": represents any number between 0 and 255. For example, 10.8.8.* denotes all addresses between 10.8.8.0 and 10.8.8.255.</li> </ul> </li> </ul>
Web: Port EMS: Destination Port CLI: dst-port <b>[PREFIX_DestPort]</b>	Defines the destination port to where you want to route the call.
Web/EMS: Transport Type CLI: transport-type <b>[PREFIX_TransportType]</b>	<p>Defines the transport layer type for sending the IP call:</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured</li> <li>▪ <b>[0]</b> UDP</li> <li>▪ <b>[1]</b> TCP</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[2] TLS</b></li> </ul> <p><b>Note:</b> When set to Not Configured (-1), the transport type defined by the SIPTransportType parameter is used.</p>
Web: Dest IP Group ID EMS: Destination IP Group ID CLI: dst-ip-group-id <b>[PREFIX_DestIPGroupID]</b>	<p>Defines the IP Group to where you want to route the call. The SIP INVITE message is sent to the IP address defined for the Proxy Set ID associated with the IP Group.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If you select an IP Group, you do not need to configure a destination IP address. However, if both parameters are configured in this table, the INVITE message is sent only to the IP Group (and not the defined IP address).</li> <li>▪ If the destination is a User-type IP Group, the device searches for a match between the Request-URI (of the received INVITE) to an AOR registration record in the device's database. The INVITE is then sent to the IP address of the registered contact.</li> <li>▪ If the parameter AlwaysUseRouteTable is set to 1 (see 'Configuring IP Groups' on page 204), then the Request-URI host name in the INVITE message is set to the value defined for the parameter 'Dest. IP Address' (above); otherwise, if no IP address is defined, it is set to the value of the parameter 'SIP Group Name' (defined in the IP Group table).</li> <li>▪ This parameter is used as the 'Serving IP Group' in the Account table for acquiring authentication user/password for this call (see 'Configuring Account Table' on page 219).</li> <li>▪ For defining Proxy Set ID's, see 'Configuring Proxy Sets Table' on page 213.</li> </ul>
Dest SRD CLI: dst-srd <b>[PREFIX_DestSRD]</b>	<p>Defines the SRD to where you want to route the call. The actual destination is defined by the Proxy Set associated with the SRD. This allows you to route the call to a specific SIP Media Realm and SIP Interface.</p> <p>To configure SRD's, see Configuring SRD Table on page 199.</p>
IP Profile ID CLI: ip-profile-id <b>[PREFIX_ProfileID]</b>	<p>Assigns an IP Profile ID to this IP destination call. This allows you to assign numerous configuration attributes (e.g., voice codes) per routing rule. To configure IP Profiles, see 'Configuring IP Profiles' on page 239.</p>
<b>Status</b>	<p>Displays the connectivity status of the routing rule's IP destination. If there is connectivity with the destination, this field displays "OK" and the device uses this routing rule if required.</p> <p>The routing rule is not used if any of the following is displayed:</p> <ul style="list-style-type: none"> <li>▪ "n/a" = The destination IP Group is unavailable</li> <li>▪ "No Connectivity" = No connection with the destination (no response to the SIP OPTIONS).</li> <li>▪ "QoS Low" = Poor Quality of Service (QoS) of the destination.</li> <li>▪ "DNS Error" = No DNS resolution. This status is applicable only when a domain name is used (instead of an IP address).</li> <li>▪ "Unavailable" = The destination is unreachable due to networking issues.</li> </ul>
Web/EMS: Charge Code CLI: charge-code <b>[PREFIX_MeteringCode]</b>	<p>Assigns a Charge Code to the routing rule. To configure Charge Codes, see Configuring Charge Codes Table on page 393.</p> <p><b>Note:</b> This parameter is applicable only to FXS interfaces.</p>
Cost Group ID CLI: cost-group-id <b>[PREFIX_CostGroupID]</b>	<p>Assigns a Cost Group with the routing rule for determining the cost of the call. To configure Cost Groups, see 'Configuring Cost Groups' on page 193.</p>

Parameter	Description
p]	
Forking Group CLI: forking-group [PREFIX_ForkingGroup]	<p>Defines a forking group ID for the routing rule. This enables forking of incoming Tel calls to two or more IP destinations. The device sends simultaneous INVITE messages and handles multiple SIP dialogs until one of the calls is answered. When a call is answered, the other calls are dropped.</p> <p>If all matched routing rules belong to the same Forking Group number, the device sends an INVITE to all the destinations belonging to this group and according to the following logic:</p> <ul style="list-style-type: none"> <li>▪ If matched routing rules belong to different Forking Groups, the device sends the call to the Forking Group of the first matched routing rule. If the call cannot be established with any of the destinations associated with this Forking Group and alternative routing is enabled, the device forks the call to the Forking Group of the next matched routing rules as long as the Forking Group is defined with a <b>higher</b> number than the previous Forking Group. For example:</li> <li>▪ Table index entries 1 and 2 are defined with Forking Group "1", and index entries 3 and 4 with Forking Group "2": The device first sends the call according to index entries 1 and 2, and if unavailable and alternative routing is enabled, sends the call according to index entries 3 and 4.</li> <li>▪ Table index entry 1 is defined with Forking Group "2", and index entries 2, 3, and 4 with Forking Group "1": The device sends the call according to index entry 1 only and ignores the other index entries even if the destination is unavailable and alternative routing is enabled. This is because the subsequent index entries are defined with a Forking Group number that is lower than that of index entry 1.</li> <li>▪ Table index entry 1 is defined with Forking Group "1", index entry 2 with Forking Group "2", and index entries 3 and 4 with Forking Group "1": The device first sends the call according to index entries 1, 3, and 4 (all belonging to Forking Group "1"), and if the destination is unavailable and alternative routing is enabled, the device sends the call according to index entry 2.</li> <li>▪ Table index entry 1 is defined with Forking Group "1", index entry 2 with Forking Group "3", index entry 3 with Forking Group "2", and index entry 4 with Forking Group "1": The device first sends the call according to index entries 1 and 4 (all belonging to Forking Group "1"), and if the destination is unavailable and alternative routing is enabled, the device sends the call according to index entry 2 (Forking Group "3"). Even if index entry 2 is unavailable and alternative routing is enabled, the device ignores index entry 3 because it belongs to a Forking Group that is lower than index entry 2.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To enable Tel-to-IP call forking, set the 'Tel2IP Call Forking Mode' (<i>Tel2IPCallForkingMode</i>) parameter to <b>Enable</b>.</li> <li>▪ You can implement Forking Groups when the destination is an LDAP server or a domain name using DNS. In such scenarios, the INVITE is sent to all the queried LDAP or resolved IP addresses respectively. You can also use LDAP routing rules with standard routing rules for Forking Groups.</li> <li>▪ When the UseDifferentRTPportAfterHold parameter is enabled, every forked call is sent with a different RTP port. Thus, ensure that the device has available RTP ports for these forked calls.</li> </ul>

## 28.3 Configuring Inbound IP Routing Table

The Inbound IP Routing Table page allows you to configure up to 24 inbound call routing rules:

- For IP-to-IP routing: The table is used to identify an incoming call as an IP-to-IP call and subsequently, to assign the call to an IP Group, referred to as a source IP Group. These IP-to-IP calls can later be routed to an outbound destination IP Group (see [Configuring Outbound IP Routing Table](#) on page 321).
- For IP-to-Tel routing: This table is used to route incoming IP calls to Trunk Groups. The specific channel pertaining to the Trunk Group to which the call is routed is determined according to the Trunk Group's channel selection mode. The channel selection mode can be defined per Trunk Group (see 'Configuring Hunt Group Settings' on page 291) or for all Trunk Groups using the global parameter `ChannelSelectMode`.

The Inbound IP Routing Table provides two configuration areas:

- Matching characteristics of incoming IP call, for example, prefix of destination number.
- Operation (destination), for example, sends to a specific Trunk Group.

If the incoming call matches the characteristics of a rule, then the call is sent to the destination configured for that rule.

The device also supports alternative routing if the Trunk Group is unavailable:

- If a call release reason is received for a specific IP-to-Tel call and this reason is configured for alternative IP-to-Tel routing, then the device re-routes the call to an alternative Trunk Group. The alternative route is configured in this table as an additional row (below the main routing rule) with the same call characteristics, but with a destination to a different Trunk Group. For more information on IP-to-Tel alternative routing, see 'Alternative Routing to Trunk upon Q.931 Call Release Cause Code' on page 339.
- The device can re-route (i.e., call redirection) IP-to-Tel calls to an alternative IP destination using SIP 3xx responses. For more information, see 'Alternative Routing to IP Destinations upon Busy Trunk' on page 340.

The device automatically re-routes an IP-to-Tel call to a different physical FXO port or physical trunk if the initially destined FXO port or physical trunk within the same Trunk Group is detected as out of service (e.g., physically disconnected). When the physical FXO port or physical trunk is disconnected, the device sends the SNMP trap, `GWAPP_TRAP_BUSYOUT_LINK` notifying of the out-of-service state for the specific FXO line or trunk number. When the FXO port or physical trunk is physically reconnected, this trap is sent notifying of the back-to-service state.



**Note:** You can also configure the Inbound IP Routing Table using the table ini file parameter, `PSTNPrefix` (see 'Number Manipulation Parameters' on page 859) or CLI command, `configure voip > gw routing ip2tel-routing`.

➤ **To configure IP-to-Tel or inbound IP routing rules:**

1. Open the Inbound IP Routing Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** > **IP to Trunk Group Routing**).

**Figure 28-3: Inbound IP Routing Table**

<div> <div>Routing Index</div> <div>1-12</div> </div> <div> <div>IP To Tel Routing Mode</div> <div>Route calls before manipulation</div> </div>								
	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IPGroup ID
1			1x	*		1	2	-1
2			[501-502]	101		2	1	
3		domain.com	*	*		3		
4			*	*	10.13.64.5	-1		4

The previous figure displays the following configured routing rules:

- **Rule 1:** If the incoming IP call destination phone prefix is between 10 and 19, the call is assigned settings configured for IP Profile ID 2 and routed to Trunk Group ID 1.
  - **Rule 2:** If the incoming IP call destination phone prefix is between 501 and 502 and source phone prefix is 101, the call is assigned settings configured for IP Profile ID 1 and routed to Trunk Group ID 2.
  - **Rule 3:** If the incoming IP call has a From URI host prefix as domain.com, the call is routed to Trunk Group ID 3.
  - **Rule 4:** If the incoming IP call has IP address 10.13.64.5 in the INVITE's Contact header, the call is identified as an IP-to-IP call and assigned to Source IP Group 4. This call is routed according to the outbound IP routing rules for this Source IP Group configured in the Outbound IP Routing Table.
2. Configure the routing rule, as required. For a description of the parameters, see the table below.
  3. Click **Submit** to apply your changes.

**IP-to-Tel or Inbound IP Routing Table Description**

Parameter	Description
IP to Tel Routing Mode CLI: configure voip/gw routing general-setting/ip2tel-rte-mode [RouteModelIP2Tel]	Determines whether to route the incoming IP call before or after manipulation of destination number, configured in 'Configuring Source/Destination Number Manipulation' on page 297. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Route calls before manipulation = (Default) Incoming IP calls are routed before number manipulation.</li> <li>▪ <b>[1]</b> Route calls after manipulation = Incoming IP calls are routed after number manipulation.</li> </ul>
<b>Matching Characteristics</b>	
Web: Dest. Host Prefix CLI: dst-phone-prefix [DestPrefix]	Defines the Request-URI host name prefix of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty. <b>Note:</b> The asterisk (*) wildcard can be used to depict any prefix.



Parameter	Description
Web: Source Host Prefix CLI: src-host-prefix <b>[SrcHostPrefix]</b>	<p>Defines the From URI host name prefix of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The asterisk (*) wildcard can be used to depict any prefix.</li> <li>If the P-Asserted-Identity header is present in the incoming INVITE message, then the value of this parameter is compared to the P-Asserted-Identity URI host name (and not the From header).</li> </ul>
Web: Dest. Phone Prefix CLI: dst-host-prefix <b>[DestHostPrefix]</b>	<p>Defines the prefix or suffix of the called (destined) telephone number. You can use special notations for denoting the prefix. For example, <b>[100-199]</b>(100,101,105) denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. To denote any prefix, use the asterisk (*) symbol or to denote calls without a called number, use the \$ sign. For a description of available notations, see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 659.</p> <p>The prefix can include up to 49 digits.</p>
Web: Source Phone Prefix CLI: src-phone-prefix <b>[SourcePrefix]</b>	<p>Defines the prefix or suffix of the calling (source) telephone number. You can use special notations for denoting the prefix. For example, <b>[100-199]</b>(100,101,105) denotes a number that starts with 100 to 199 and ends with 100, 101 or 105. To denote any prefix, use the asterisk (*) symbol or to denote calls without a calling number, use the \$ sign. For a description of available notations, see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 659.</p> <p>The prefix can include up to 49 digits.</p>
Web: Source IP Address CLI: src-ip-address <b>[SourceAddress]</b>	<p>Defines the source IP address of the incoming IP call that can be used for routing decisions.</p> <p>The IP address can be configured in dotted-decimal notation (e.g., 10.8.8.5) or as an FQDN. If the address is an FQDN, DNS resolution is done according to the DNSQueryType parameter.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The source IP address is obtained from the Contact header in the INVITE message.</li> <li>You can configure from where the source IP address is obtained, using the SourceIPAddressInput parameter.</li> <li>The source IP address can include the following wildcards: <ul style="list-style-type: none"> <li>✓ "x": denotes single digits. For example, 10.8.8.xx represents all the addresses between 10.8.8.10 and 10.8.8.99.</li> <li>✓ "**": denotes any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255.</li> </ul> </li> </ul>
Source SRD ID CLI: src-srd-id <b>[SrcSRDID]</b>	<p>Defines the SRD from which the incoming packet is received.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>When the incoming INVITE matches the SRD in the routing rule, if the 'Source IP Group ID' parameter (see below) is defined and it is associated with a different SRD, the incoming SIP call is rejected. If the 'Source IP Group ID' parameter is not defined, the SRD's default IP Group is used. If there is no valid source IP Group, the call is rejected.</li> <li>Currently, this parameter can only be configured using the ini file.</li> </ul>



Parameter	Description
<b>Operation (Destination)</b>	
Web: Trunk Group ID CLI: trunk-group-id <b>[TrunkGroupId]</b>	For IP-to-Tel calls: Defines the Trunk Group to where the incoming SIP call is sent. For IP-to-IP calls: Identifies the call as an IP-to-IP call if this parameter is set to -1.
Web: Trunk ID CLI: trunk-id <b>[TrunkId]</b>	Defines the Trunk to where the incoming SIP call is sent. <b>Notes:</b> <ul style="list-style-type: none"> <li>If both 'Trunk Group ID' and 'Trunk ID' parameters are configured in the table, the routing is done according to the 'Trunk Group ID' parameter.</li> <li>The method for selecting the trunk's channel to which the IP call is sent is configured by the global parameter, ChannelSelectMode.</li> <li>Currently, this field can only be configured using the ini file.</li> </ul>
Web: IP Profile ID CLI: ip-profile-id <b>[ProfileId]</b>	Assigns an IP Profile (configured in 'Configuring IP Profiles' on page <a href="#">239</a> ) to the call.
Web: Source IP Group ID CLI: src-ip-group-id <b>[SrcIPGroupID]</b>	For IP-to-Tel calls: Defines the IP Group associated with the incoming IP call. This is the IP Group that sent the INVITE message. This IP Group can later be used as the 'Serving IP Group' in the Account table for obtaining authentication user name/password for this call (see 'Configuring Account Table' on page <a href="#">219</a> ). For IP-to-IP calls: Assigns the IP Group to the incoming IP call. This IP Group can later be used for outbound IP routing and as the 'Serving IP Group' in the Account table for obtaining authentication user name/password for this call (see Configuring Account Table on page <a href="#">219</a> ).

## 28.4 IP Destinations Connectivity Feature

The device can be configured to check the integrity of the connectivity to IP destinations of Tel-to-IP routing rules in the Outbound IP Routing table. The IP Connectivity feature can be used for the Alternative Routing feature, whereby the device attempts to re-route calls from unavailable Tel-to-IP routing destinations to available ones (see 'Alternative Routing Based on IP Connectivity' on page 335).

The device supports the following methods for checking the connectivity of IP destinations:

- **Network Connectivity:** The device checks the network connectivity of the IP destination configured by the 'Alt Routing Tel to IP Connectivity Method' parameter:
  - **SIP OPTIONS:** The device sends "keep-alive" SIP OPTIONS messages to the IP destination. If the device receives a SIP 200 OK in response, it considers the destination as available. If the destination does not respond to the OPTIONS message, then it is considered unavailable. You can configure the time interval for sending these OPTIONS messages, using the 'Alt Routing Tel to IP Keep Alive Time' parameter.

These parameters are configured in the Routing General Parameters page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **General Parameters**), as shown below:

**Figure 28-4: IP Connectivity Method in Routing General Parameters Page**

Alt Routing Tel to IP Connectivity Method	SIP OPTIONS
Alt Routing Tel to IP Keep Alive Time	60

- **Quality of Service (QoS):** You can enable the device to check the QoS of IP destinations. The device measures the QoS according to RTCP statistics of previously established calls with the IP destination. The RTCP includes packet delay (in milliseconds) and packet loss (in percentage). If these measured statistics exceed a user-defined threshold, the destination is considered unavailable. Note that if call statistics is not received within two minutes, the QoS data is reset. These thresholds are configured using the following parameters:
  - 'Max Allowed Packet Loss for Alt Routing' (IPConnQoSMaxAllowedPL): defines the threshold value for packet loss after which the IP destination is considered unavailable.
  - 'Max Allowed Delay for Alt Routing' (IPConnQoSMaxAllowedDelay): defines the threshold value for packet delay after which the IP destination is considered unavailable

These parameters are configured in the Routing General Parameters page, as shown below:

**Figure 28-5: IP QoS Thresholds in Routing General Parameters Page**

Max Allowed Packet Loss for Alt Routing [%]	20
Max Allowed Delay for Alt Routing [msec]	250

- **DNS Resolution:** When a host name (FQDN) is used (instead of an IP address) for the IP destination, it is resolved into an IP address by a DNS server. The device checks network connectivity and QoS of the resolved IP address. If the DNS host name is unresolved, the device considers the connectivity of the IP destination as unavailable.

You can view the connectivity status of IP destinations in the following Web interface pages:

- **Outbound IP Routing Table:** The connectivity status of the IP destination per routing rule is displayed in the 'Status' column. For more information, see 'Configuring Outbound IP Routing Table' on page 321.
- **IP Connectivity:** This page displays a more informative connectivity status of the IP destinations used in Tel-to-IP routing rules in the Outbound IP Routing table. For viewing this page, see 'Viewing IP Connectivity' on page 597.

## 28.5 Alternative Routing for Tel-to-IP Calls

The device supports various alternative Tel-to-IP call routing methods, as described in this section.

### 28.5.1 Alternative Routing Based on IP Connectivity

You can configure the device to do alternative Tel-to-IP call routing based on IP connectivity. When the connectivity state of an IP destination is unavailable, the device attempts to re-route the Tel-to-IP call to an alternative IP destination. It does this by searching for the next call matching rule (e.g., phone number prefix) in the Outbound IP Routing table.

The device searches for an alternative IP destination when any of the following connectivity states are detected with the IP destination of the initial Tel-to-IP routing rule:

- No response received from SIP OPTIONS messages. This depends on the chosen method for checking IP connectivity.
- Poor QoS according to the configured thresholds for packet loss and delay.
- Unresolved DNS, if the configured IP destination is a domain name (or FQDN). If the domain name is resolved into two IP addresses, the timeout for INVITE re-transmissions can be configured using the HotSwapRtx parameter. For example, if you set this parameter to 3, the device attempts up to three times to route the call to the first IP address and if unsuccessful, it attempts up to three times to re-route it to the second resolved IP address.

The connectivity status of the IP destination is displayed in the 'Status' column of the Outbound IP Routing table per routing rule. If it displays a status other than "ok", then the device considers the IP destination as unavailable and attempts to re-route the call to an alternative destination. For more information on the IP connectivity methods and on viewing IP connectivity status, see 'IP Destinations Connectivity Feature' on page 334.

The table below shows an example of alternative routing where the device uses an available alternative routing rule in the Outbound IP Routing table to re-route the initial Tel-to-IP call.

**Alternative Routing based on IP Connectivity Example**

	Destination Phone Prefix	IP Destination	IP Connectivity Status	Rule Used?
Main Route	40	10.33.45.68	"No Connectivity"	No
Alternative Route #1	40	10.33.45.70	"QoS Low"	No
Alternative Route #2	40	10.33.45.72	"ok"	Yes


**Notes:**

- Alternative routing based on IP connectivity is applicable only when a proxy server is not used.
- As the device searches the Outbound IP Routing table for a matching rule starting from the top, you must configure the main routing rule above the alternative routing rules.
- You can configure up to two alternative routing rules.
- For configuring Tel-to-IP routing rules in the Outbound IP Routing table, see 'Configuring Outbound IP Routing Table' on page 321.

The steps for configuring alternative Tel-to-IP routing based on IP connectivity are summarized below.

➤ **To configure alternative Tel-to-IP routing based on IP connectivity:**

1. In the Outbound IP Routing table, add alternative Tel-to-IP routing rules for specific calls.
2. In the Routing General Parameters page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **General Parameters**), do the following:
  - a. Enable alternative routing based on IP connectivity, by setting the 'Enable Alt Routing Tel to IP AltRouting' (Tel2IPEnable) parameter to **Enable**.
  - b. Configure the IP connectivity reason for triggering alternative routing, by setting the 'Alt Routing Tel to IP Mode' parameter (AltRoutingTel2IPMode) to one of the following:
    - ◆ SIP OPTIONS failure
    - ◆ Poor QoS
    - ◆ SIP OPTIONS failure, poor QoS, or unresolved DNS
  - c. The device plays a tone to the Tel endpoint (for analog interfaces) whenever an alternative route is used. This tone is played for a user-defined time configured by the 'Alternative Routing Tone Duration' parameter.

## 28.5.2 Alternative Routing Based on SIP Responses

You can configure the device to do alternative routing based on the received SIP response. If the SIP response code reflects an error (i.e., 4xx, 5xx, or 6xx) and you have configured this specific response code as a trigger for alternative routing, then the device attempts to re-route the call to an alternative destination.

You can configure up to five SIP response codes for triggering alternative routing. This is done in the Reasons for Alternative Routing table, explained in this section.

Typically, the device performs alternative routing when there is no response at all to an INVITE message after a user-defined number of INVITE re-transmissions, configured using the SIPMaxRtx parameter. In such a scenario, the device issues itself the SIP response code 408 "Request Timeout". If this release code is defined in the Reasons for Alternative Routing table, then alternative routing is done.



**Note:** The device also plays a tone to the endpoint whenever an alternative route is used. This tone is played for a user-defined time, configured by the AltRoutingToneDuration parameter.

Depending on configuration, the alternative routing is done using one of the following configuration entities:

- **Outbound IP Routing Rules:** You can configure up to two alternative routing rules in the table. If the initial, main routing rule destination is unavailable, the device searches the table (starting from the top) for the next call matching rule (e.g., destination phone number), and if available attempts to re-route the call to the IP destination configured for this alternative routing rule. The table below shows an example of alternative routing where the device uses the first available alternative routing rule to re-route the initial, unsuccessful Tel-to-IP call destination.

**Alternative Routing based on SIP Response Code Example**

	Destination Phone Prefix	IP Destination	SIP Response	Rule Used?
Main Route	40	10.33.45.68	408 Request Timeout	No
Alternative Route #1	40	10.33.45.70	486 Busy Here	No
Alternative Route #2	40	10.33.45.72	200 OK	Yes

- **Proxy Sets:** Proxy Sets are used for Server-type IP Groups (e.g., an IP PBX) and define the actual IP destination (IP address or FQDN) of the server. As you can define up to five IP destinations per Proxy Set, the device supports proxy redundancy, which works together with the alternative routing feature. If the destination of a routing rule in the Outbound IP Routing table is an IP Group, the device routes the call to the IP destination configured for the Proxy Set associated with the IP Group. If the first IP destination of the Proxy Set is unavailable, the device attempts to re-route the call to the next proxy destination, and so on until an available IP destination is located. To enable the Proxy Redundancy feature, set the IsProxyHotSwap parameter to 1 (per Proxy Set) and set the EnableProxyKeepAlive to 1.

When the Proxy Redundancy feature is enabled, the device continually monitors the connection with the proxies by using keep-alive messages (SIP OPTIONS). The device sends these messages every user-defined interval (ProxyKeepAliveTime parameter). Any response from the proxy, either success (200 OK) or failure (4xx response) is considered as if the proxy is communicating. If there is no response from the first (primary) proxy after a user-defined number of re-transmissions (re-INVITES) configured using the HotSwapRtx parameter, the device attempts to communicate (using the same INVITE) with the next configured (redundant) proxy in the list, and so on until an available redundant proxy is located. The device's behavior can then be one of the following, depending on the ProxyRedundancyMode parameter setting:

- The device continues operating with the redundant proxy (now active) until the next failure occurs, after which it switches to the next redundant proxy. This is referred to as *Parking* mode.
- The device always attempts to operate with the primary proxy. In other words, it switches back to the primary proxy whenever it's available again. This is referred to as *Homing* mode.

If none of the proxy servers respond, the device goes over the list again.

The steps for configuring alternative Tel-to-IP routing based on SIP response codes are summarized below.

➤ **To configure alternative Tel-to-IP routing based on SIP response codes:**

1. Enable alternative routing based on SIP responses, by setting the 'Redundant Routing Mode' parameter to one of the following:
  - **Routing Table** for using the Outbound IP Routing table for alternative routing.
  - **Proxy** for using the Proxy Set redundancy feature for alternative routing.
2. If you are using the Outbound IP Routing table, configure alternative routing rules with identical call matching characteristics, but with different IP destinations. If you are using the Proxy Set, configure redundant proxies.
3. Define SIP response codes (call failure reasons) that invoke alternative Tel-to-IP routing:
  - a. Open the Reasons for Alternative Routing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** submenu > **Alternative Routing Reasons**).

**Figure 28-6: Tel to IP Reasons - Reasons for Alternative Routing Page**

Tel to IP Reasons	
Reason 1	▼
Reason 2	▼
Reason 3	▼
Reason 4	▼
Reason 5	▼

- b. Under the 'Tel to IP Reasons' group, select up to five different SIP response codes (call failure reasons) that invoke alternative Tel-to-IP routing.
- c. Click **Submit**.

### 28.5.3 PSTN Fallback

The PSTN Fallback feature enables the device to re-route a Tel-to-IP call to the legacy PSTN using one of its trunks if the IP destination is unavailable. For example, if poor voice quality is detected over the IP network, the device attempts to re-route the call to the PSTN.

The steps for configuring alternative Tel-to-IP routing to the legacy PSTN are summarized below.

➤ **To configure alternative Tel-to-IP routing to the legacy PSTN:**

1. Configure an alternative routing rule in the Outbound IP Routing table with the same call matching characteristics (e.g., phone number destination), but where the destination is the IP address of the device itself.
2. Configure an IP-to-Tel routing rule in the Inbound IP Routing table to route calls received from the device (i.e., its IP address) to a specific Trunk Group connected to the PSTN. This configuration is necessary as the re-routed call is now considered an IP-to-Tel call. For configuring IP-to-Tel routing rules, see 'Configuring the Inbound IP Routing Table' on page 330.



**Note:** The PSTN Fallback feature is applicable only to digital interfaces (e.g., E1 / T1 trunks).

## 28.6 Alternative Routing for IP-to-Tel Calls

The device supports alternative IP-to-Tel call routing, as described in this section.

### 28.6.1 Alternative Routing to Trunk upon Q.931 Call Release Cause Code

You can configure the device to do alternative IP-to-Tel call routing based on the received ISDN Q.931 cause code. If an IP-to-Tel call is rejected or disconnected on the Tel side as a result of a specific ISDN Q.931 release cause code that is listed in the Reasons for Alternative Routing table, the device searches for an alternative IP-to-Tel routing rule in the Inbound IP Routing table and sends it to the alternative Trunk Group. For example, you can enable alternative IP-to-Tel routing for scenarios where the initial Tel destination is busy and a Q.931 Cause Code No. 17 is received (or for other call releases that issue the default Cause Code No. 3).

You can also configure a default release cause code that the device issues itself upon the following scenarios:

- The device initiates a call release whose cause is unknown.
- No free channels (i.e., busy) in the Trunk Group.
- No appropriate routing rule located in the Inbound IP Routing table to the Trunk Group.
- Phone number is not found in the Inbound IP Routing table.

By default, it is set to Cause Code No. 3 (No Route to Destination). This default cause code can be changed using the 'Default Release Cause' parameter located in the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**). To enable alternative routing based on Q.931 cause code, you need to define this cause code in the Reasons for Alternative Routing table.

➤ **To configure alternative Trunk Group routing based on Q.931 cause codes:**

1. In the Proxy & Registration page, set the 'Redundant Routing Mode' parameter to **Routing Table** so that the device uses the Inbound IP Routing table for alternative routing.
2. In the Inbound IP Routing table, configure alternative routing rules with the same call matching characteristics, but with different Trunk Group destinations.
3. Configure up to five Q.931 cause codes that invoke alternative IP-to-Tel routing:
  - a. Open the Reasons for Alternative Routing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **Alternative Routing Reasons**).

**Figure 28-7: IP to Tel Reasons - Reasons for Alternative Routing Page**

IP to Tel Reasons	
Reason 1	3 ▼
Reason 2	17 ▼
Reason 3	▼
Reason 4	▼
Reason 5	▼

- b. Under the 'IP to Tel Reasons' group, select the desired Q.931 cause codes.
- c. Click **Submit** to apply your changes.




**Notes:**

- You can configure up to two alternative routing rules in the Inbound IP Routing table.
- If a Trunk is disconnected or not synchronized, the device issues itself the internal Cause Code No. 27. This cause code is mapped (by default) to SIP 502.
- The default release cause is described in the Q.931 notation and is translated to corresponding SIP 40x or 50x values (e.g., Cause Code No. 3 to SIP 404, and Cause Code No. 34 to SIP 503).
- For analog interfaces: For information on mapping PSTN release causes to SIP responses, see PSTN Release Cause to SIP Response Mapping on page 318.
- For mapping SIP-to-Q.931 and Q.931-to-SIP release causes, see Configuring Release Cause Mapping on page 313.
- For configuring IP-to-Tel routing rules in the Inbound IP Routing table, see 'Configuring Inbound IP Routing Table' on page 330.
- The Reasons for Alternative Routing IP to Tel table can also be configured using the table ini file parameter, AltRouteCauseIP2Tel or CLI command, configure voip/gw routing alt-route-cause-ip2tel.

## 28.6.2 Alternative Routing to an IP Destination upon a Busy Trunk

You can configure the device to forward (i.e., call redirection) IP-to-Tel calls to an alternative IP destination using SIP 3xx responses. This can be done upon the following scenarios:

- For digital interfaces: Trunk Group has no free channels (i.e., “busy”).
- For analog interfaces: Unavailable FXS / FXO Trunk Group. This feature can be used, for example, to forward the call to another FXS / FXO device.

This feature is configured per Trunk Group and is configured in the Forward on Busy Trunk Destination table, as described in this section.

The alternative destination can be defined as a host name or as a SIP Request-URI user name and host part (i.e., user@host). For example, the below configuration forwards IP-to-Tel calls to destination user “112” at host IP address 10.13.4.12, port 5060, using transport protocol TCP, if Trunk Group ID 2 is unavailable:

```
ForwardOnBusyTrunkDest 1 = 2, 112@10.13.4.12:5060;transport=tcp;
```

When configured with user@host, the original destination number is replaced by the user part.

The device forwards calls using this table only if no alternative IP-to-Tel routing rule has been configured in the Inbound IP Routing table or alternative routing fails and one of the following reasons included in the SIP Diversion header of 3xx messages exists:

- For digital interfaces: “out-of-service” - all trunks are unavailable/disconnected
- “unavailable”:
  - For digital interfaces: All trunks are busy or unavailable
  - For analog interfaces: All FXS / FXO lines pertaining to a Trunk Group are busy or unavailable



**Note:** You can also configure the Forward on Busy Trunk Destination table using the table ini file parameter, ForwardOnBusyTrunkDest or CLI command, configure voip/gw routing fwd-on-busy-trk-dst.



➤ **To configure Forward on Busy Trunk Destination rules:**

1. Open the Forward on Busy Trunk Destination page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **Forward on Busy Trunk**).

**Figure 28-8: Forward on Busy Trunk Destination Page**

Index	Trunk Group ID	Forward Destination
0 <input type="radio"/>	<input type="text" value="1"/>	<input type="text" value="10.13.5.67"/>

The figure above displays a configuration that forwards IP-to-Tel calls destined for Trunk Group ID 1 to destination IP address 10.13.5.67 if the conditions mentioned earlier exist.

2. Configure the table as required, and then click **Submit** to apply your changes.
3. Save the changes to the device's flash memory with a device reset (see 'Saving Configuration' on page 532).

**Forward on Busy Trunk Destination Description Parameters**

Parameter	Description
Trunk Group ID CLI: trunk-group-id <b>[ForwardOnBusyTrunkDest_TrunkGroupId]</b>	Defines the Trunk Group ID to which the IP call is destined to.
Forward Destination CLI: forward-dst <b>[ForwardOnBusyTrunkDest_ForwardDestination]</b>	<p>Defines the alternative IP destination for the call used if the Trunk Group is busy or unavailable.</p> <p>The valid value can be an IP address in dotted-decimal notation, an FQDN, or a SIP Request-URI user name and host part (i.e., user@host). The following syntax can also be used: host:port;transport=xxx (i.e., IP address, port and transport type).</p> <p><b>Note:</b> When configured with a user@host, the original destination number is replaced by the user part.</p>

## Reader's Notes

## 29 Configuring DTMF and Dialing

The DTMF & Dialing page is used to configure parameters associated with dual-tone multi-frequency (DTMF) and dialing. For a description of the parameters appearing on this page, see 'Configuration Parameters Reference' on page 661.

➤ **To configure the DTMF and dialing parameters:**

1. Open the DTMF & Dialing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **DTMF & Supplementary** submenu > **DTMF & Dialing**).

Max Digits In Phone Num	<input type="text" value="30"/>
Inter Digit Timeout [sec]	<input type="text" value="4"/>
Declare RFC 2833 in SDP	<input type="text" value="Yes"/>
1st Tx DTMF Option	<input type="text" value="RFC 2833"/>
2nd Tx DTMF Option	<input type="text"/>
RFC 2833 Payload Type	<input type="text" value="96"/>
Hook-Flash Option	<input type="text" value="Not Supported"/>
Digit Mapping Rules	<input type="text"/>
Dial Plan Index	<input type="text" value="-1"/>
Dial Tone Duration [sec]	<input type="text" value="16"/>
Hotline Dial Tone Duration [sec]	<input type="text" value="16"/>
Enable Special Digits	<input type="text" value="Disable"/>
Dial Plan Index	<input type="text" value="-1"/>
Min Routing Overlap Digits	<input type="text" value="1"/>
ISDN Overlap IP to Tel Dialing	<input type="text" value="Disable"/>
Default Destination Number	<input type="text" value="1000"/>
Special Digit Representation	<input type="text" value="Special"/>

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 29.1 Dialing Plan Features

This section describes various dialing plan features supported by the device.

### 29.1.1 Digit Mapping

Digit map pattern rules are used for Tel-to-IP ISDN overlap dialing (by setting the ISDNRxOverlap parameter to 1) to reduce the dialing period (for digital interface). For more information on digit maps for ISDN overlapping, see ISDN Overlap Dialing on page 286. The device collects digits until a match is found in the user-defined digit pattern (e.g., for closed numbering schemes). The device stops collecting digits and starts sending the digits (collected number) when any one of the following scenarios occur:

- Maximum number of digits is received. You can define (using the MaxDigits parameter) the maximum number of collected destination number digits that can be received (i.e., dialed) from the Tel side by the device. When the number of collected digits reaches the maximum (or a digit map pattern is matched), the device uses these digits for the called destination number.
- Inter-digit timeout expires (e.g., for open numbering schemes). This is defined using the TimeBetweenDigits parameter. This is the time that the device waits between each received digit. When this inter-digit timeout expires, the device uses the collected digits to dial the called destination number.
- The phone's pound (#) key is pressed.
- Digit string (i.e., dialed number) matches one of the patterns defined in the digit map.

Digit map (pattern) rules are defined using the DigitMapping parameter. The digit map pattern can contain up to 52 options (rules), each separated by a vertical bar ("|"). The maximum length of the entire digit pattern is 152 characters. The available notations are described in the table below:

**Digit Map Pattern Notations**

Notation	Description
<b>[n-m]</b>	Range of numbers (not letters).
<b>.</b>	(single dot) Repeat digits until next notation (e.g., T).
<b>x</b>	Any single digit.
<b>T</b>	Dial timeout (configured by the TimeBetweenDigits parameter).
<b>S</b>	Short timer (configured by the TimeBetweenDigits parameter; default is two seconds) that can be used when a specific rule is defined after a more general rule. For example, if the digit map is 99 998, then the digit collection is terminated after the first two 9 digits are received. Therefore, the second rule of 998 can never be matched. But when the digit map is 99s 998, then after dialing the first two 9 digits, the device waits another two seconds within which the caller can enter the digit 8.

Below is an example of a digit map pattern containing eight rules:

```
DigitMapping = 11xS|00[1-7]xxx|8xxxxxxx|#xxxxxxx|*xx|91xxxxxxxxxxxx|9011x|xx.T
```

In the example, the rule "00[1-7]xxx" denotes dialed numbers that begin with 00, and then any digit from 1 through 7, followed by three digits (of any number). Once the device receives these digits, it does not wait for additional digits, but starts sending the collected digits (dialed number) immediately.

**Notes:**

- If you want the device to accept/dial any number, ensure that the digit map contains the rule "xx.T"; otherwise, dialed numbers not defined in the digit map are rejected.
- If you are using an external Dial Plan file for dialing plans (see 'Dialing Plans for Digit Collection' on page 542), the device first attempts to locate a matching digit pattern in the Dial Plan file, and if not found, then attempts to locate a matching digit pattern in the Digit Map (configured by the DigitMapping parameter).
- It may be useful to configure both Dial Plan file and Digit Maps. For example, the Digit Map can be used for complex digit patterns (which are not supported by the Dial Plan) and the Dial Plan can be used for long lists of relatively simple digit patterns. In addition, as timeout between digits is not supported by the Dial Plan, the Digit Map can be used to define digit patterns (MaxDigits parameter) that are shorter than those defined in the Dial Plan, or left at default. For example, "xx.T" Digit Map instructs the device to use the Dial Plan and if no matching digit pattern, it waits for two more digits and then after a timeout (TimeBetweenDigits parameter), it sends the collected digits. Therefore, this ensures that calls are not rejected as a result of their digit pattern not been completed in the Dial Plan.

### 29.1.2 External Dial Plan File

The device can be loaded with a Dial Plan file with user-defined dialing plans. For more information, see 'Dial Plan File' on page 541.

## Reader's Notes

## 30 Configuring Supplementary Services

This section describes SIP supplementary services that can enhance your telephone service.

**Notes:**

- All call participants must support the specific supplementary service that is used.
- When working with certain application servers (such as BroadSoft's BroadWorks) in client server mode (the application server controls all supplementary services and keypad features by itself), the device's supplementary services must be disabled.

The Supplementary Services page is used to configure many of the discussed supplementary services parameters. For a description of the parameters appearing on this page, see 'Configuration Parameters Reference' on page 661.

➤ **To configure supplementary services parameters:**

1. Open the Supplementary Services page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **DTMF & Supplementary** submenu > **Supplementary Services**).

**Figure 30-1: Supplementary Services Page**

Enable Hold	Enable
Enable Hold to ISDN	Disable
Hold Format	0.0.0.0
Held Timeout	-1
Call Hold Reminder Ring Timeout	30
Enable Transfer	Enable
Transfer Prefix	
Enable Call Forward	Enable
Enable Call Waiting	Enable
Number of Call Waiting Indications	2
Time Between Call Waiting Indications	10
Time Before Waiting Indications	0
Waiting Beep Duration	300
Enable Caller ID	Disable
Caller ID Type	Standard Bellcore
Hook-Flash Code	
Flash Keys Sequence Style	0
Flash Keys Sequence Timeout	2000
Max 3 Way Conference on Board Calls	2
Non Allocatable Ports	0
Enable NRT Subscription	Disable
AS Subscribe IPGroupID	-1
NRT Subscribe Retry Time	120
Call Forward Ring Tone ID	1

<b>MWI Parameters</b>	
Enable MWI	Disable
MWI Analog Lamp	Disable
MWI Display	Disable
Subscribe to MWI	No
MWI Server Transport Type	Not Configured
MWI Server IP Address	
MWI Subscribe Expiration Time	7200
MWI Subscribe Retry Time	120
Stutter Tone Duration	2000

<b>Conference</b>	
Enable 3-Way Conference	Disable
Establish Conference Code	!
Conference ID	conf
Three Way Conference Mode	AudioCodes Media Server

<b>MLPP</b>	
Call Priority Mode	Disable
MLPP Diffserv	50
Precedence Ringing Type	-1

<b>BRI to SIP Supplementary Services Codes</b>	
Call Forward Unconditional	
Call Forward Unconditional Deactivation	
Call Forward on Busy	
Call Forward on Busy Deactivation	
Call Forward on No Reply	
Call Forward on No Reply Deactivation	

<b>Transfer</b>	
Blind	

2. Configure the parameters as required.
3. Click **Submit** to apply your changes, or click the **Subscribe to MWI** or **Unsubscribe to MWI** buttons to save your changes and to subscribe / unsubscribe to the MWI server.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.



## 30.1 Call Hold and Retrieve

Initiating Call Hold and Retrieve:

- Active calls can be put on-hold by pressing the phone's hook-flash button.
- The party that initiates the hold is called the *holding* party; the other party is called the *held* party.
- After a successful Hold, the holding party hears a dial tone (HELD\_TONE defined in the device's Call Progress Tones file).
- Call retrieve can be performed only by the holding party while the call is held and active.
- The holding party performs the retrieve by pressing the telephone's hook-flash button.
- After a successful retrieve, the voice is connected again.
- Hold is performed by sending a Re-INVITE message with IP address 0.0.0.0 or a=sendonly in the SDP according to the parameter HoldFormat.
- The hold and retrieve functionalities are implemented by re-INVITE messages. The IP address 0.0.0.0 as the connection IP address or the string 'a=inactive' in the received re-INVITE SDP cause the device to enter Hold state and to play the held tone (configured in the device) to the PBX/PSTN. If the string 'a=sendonly' is received in the SDP message, the device stops sending RTP packets, but continues to listen to the incoming RTP packets. Usually, the remote party plays, in this scenario, Music on Hold (MOH) and the device forwards the MOH to the held party.

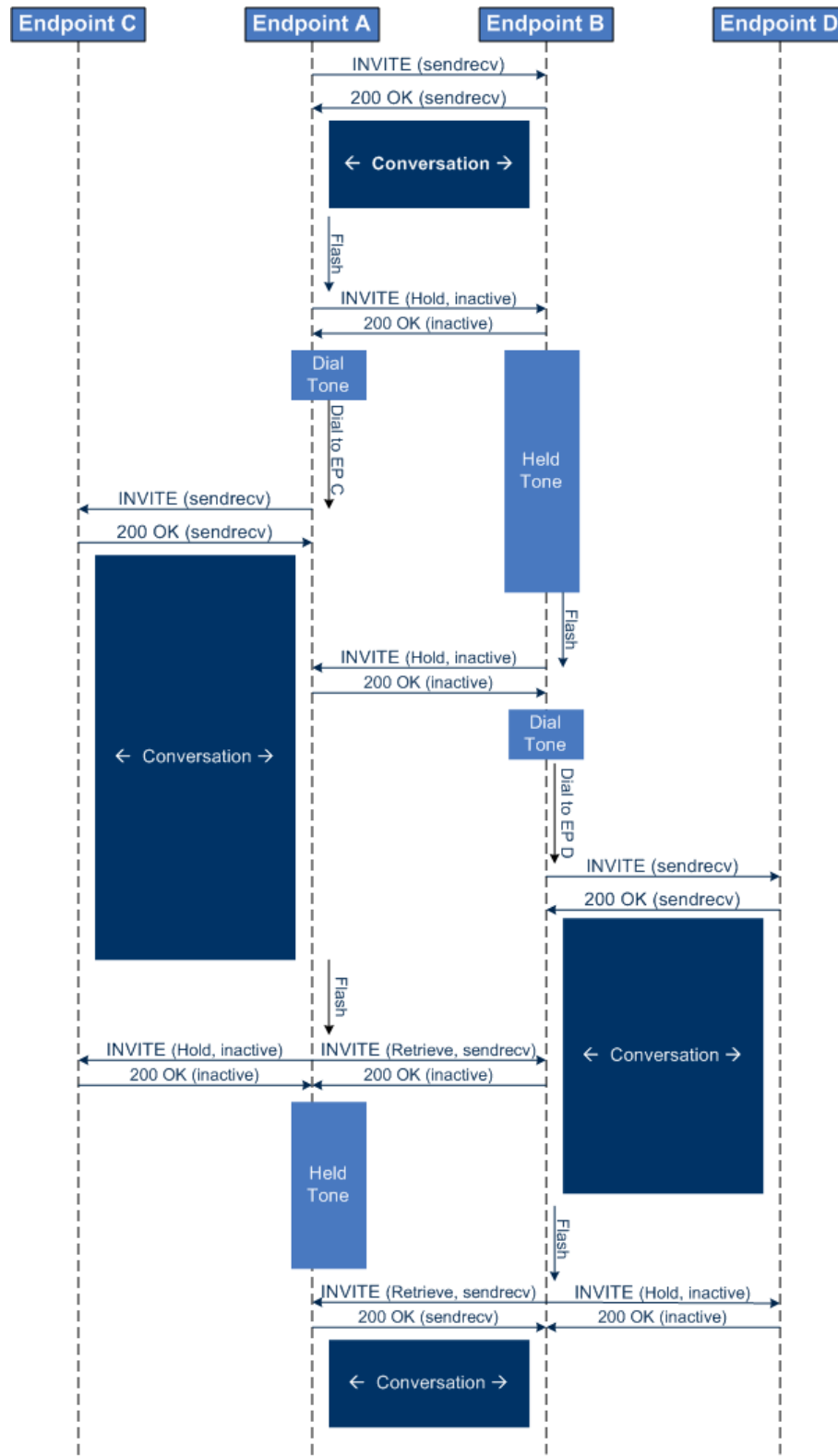
Receiving Hold/Retrieve:

- When an active call receives a re-INVITE message with either the IP address 0.0.0.0 or the 'inactive' string in SDP, the device stops sending RTP and plays a local held tone.
- When an active call receives a re-INVITE message with the 'sendonly' string in SDP, the device stops sending RTP and listens to the remote party. In this mode, it is expected that on-hold music (or any other hold tone) is played (over IP) by the remote party.

You can also configure the device to keep a call on-hold for a user-defined time after which the call is disconnected, using the HeldTimeout parameter.

The device also supports "double call hold" for FXS interfaces where the called party, which has been placed on-hold by the calling party, can then place the calling party on hold as well and make a call to another destination. The flowchart below provides an example of this type of call hold:

**Figure 30-2: Double Hold SIP Call Flow**



The flowchart above describes the following "double" call-hold scenario:

1. A calls B and establishes a voice path.
2. A places B on hold; A hears a dial tone and B hears a held tone.
3. A calls C and establishes a voice path.
4. B places A on hold; B hears a dial tone.
5. B calls D and establishes a voice path.
6. A ends call with C; A hears a held tone.
7. B ends call with D.
8. B retrieves call with A.



**Notes:**

- If a party that is placed on hold (e.g., B in the above example) is called by another party (e.g., D), then the on-hold party receives a call waiting tone instead of the held tone.
- While in a Double Hold state, placing the phone on-hook disconnects both calls (i.e. call transfer is not performed).
- You can enable the device to handle incoming re-INVITE messages with "a=sendonly" in the SDP, in the same way as if "a=inactive" is received in the SDP. This is configured using the SIPHoldBehavior parameter. When enabled, the device plays a held tone to the Tel phone and responds with a 200 OK containing "a=recvonly" in the SDP.

## 30.2 Call Pickup

The device supports the Call Pick-Up feature, whereby the FXS user can answer someone else's telephone call by pressing a user-defined sequence of phone keys. When the user dials the user-defined digits (e.g., #77), the incoming call from the other phone is forwarded to the FXS user's phone. This feature is configured using the parameter KeyCallPickup.



**Note:** The Call Pick-Up feature is supported only for FXS endpoints pertaining to the same Trunk Group ID.

## 30.3 BRI Suspend and Resume

The device supports call suspend and resume services initiated by ISDN BRI phones connected to the device. During an ongoing call, the BRI phone user can suspend the call by typically pressing the phone's "P" button or a sequence of keys (depending on the phone), and then on-hooking the handset. To resume the call, the phone user typically presses the same keys or button again and then off-hooks the phone. During the suspended state, the device plays a howler tone to the remote party. This service is also supported when instead of pressing the call park button(s), the phone cable is disconnected (suspending the call) and then reconnected again (resuming the call).

If the phone user does not resume the call within a user-defined interval (configured using the HeldTimeout parameter), the device releases the call.



**Note:** Only one call can be suspended per trunk. If another suspend request is received from a BRI phone while there is already a suspended call (even if done by another BRI phone connected to the same trunk), the device rejects this suspend request.

## 30.4 Consultation Feature

The device's Consultation feature allows you to place one number on hold and make a second call to another party.

- After holding a call (by pressing hook-flash), the holding party hears a dial tone and can then initiate a new call, which is called a Consultation call.
- While hearing a dial tone, or when dialing to the new destination (before dialing is complete), the user can retrieve the held call by pressing hook-flash.
- The held call can't be retrieved while ringback tone is heard.
- After the Consultation call is connected, the user can toggle between the held and active call by pressing the hook-flash key.



**Note:** The Consultation feature is applicable only to FXS interfaces.

## 30.5 Call Transfer

This section describes the device's support for call transfer types.

### 30.5.1 Consultation Call Transfer

The device supports Consultation Call Transfer using the SIP REFER message and Replaces header. The common method to perform a consultation transfer is described in the following example, which assumes three call parties:

- Party A = transferring
  - Party B = transferred
  - Party C = transferred to
1. A Calls B.
  2. B answers.
  3. A presses the hook-flash button and places B on-hold (party B hears a hold tone).
  4. A dials C.
  5. After A completes dialing C, A can perform the transfer by on-hooking the A phone.
  6. After the transfer is complete, B and C parties are engaged in a call.

The transfer can be initiated at any of the following stages of the call between A and C:

- Just after completing dialing C phone number - transfer from setup
- While hearing ringback – transfer from alert
- While speaking to C - transfer from active



**Note:** For FXS interfaces, the device can also handle call transfers using SIP INVITE and re-INVITE messages, instead of REFER messages. This is useful when communicating with SIP UAs that do not support the receipt of REFER messages. This feature is applicable to FXS interfaces. To enable this support, use the EnableCallTransferUsingReinvites parameter.

The device also supports attended (consultation) call transfer for BRI phones (user side) connected to the device and using the Euro ISDN protocol. BRI call transfer is according to ETSI TS 183 036, Section G.2 (Explicit Communication Transfer – ECT). Call transfer is enabled using the EnableTransfer and EnableHoldtoISDN parameters.

The Explicit Call Transfer (ECT, according to ETS-300-367, 368, 369) supplementary service is supported for BRI and PRI trunks. This service provides the served user who has two calls to ask the network to connect these two calls together and release its connection to both parties. The two calls can be incoming or outgoing calls. This service is similar to NI2 Two B-Channel Transfer (TBCT) Supplementary Service. The main difference is that in ECT one of the calls must be in HELD state. The ECT standard defines two methods - Implicit and Explicit. In implicit method, the two calls must be on the same trunk. BRI uses the implicit mechanism, and PRI the explicit mechanism.

### 30.5.2 Consultation Transfer for QSIG Path Replacement

The device can interwork consultation call transfer requests for ISDN QSIG-to-IP calls. When the device receives a request for a consultation call transfer from the PBX, the device sends a SIP REFER message with a Replaces header to the SIP UA to transfer it to another SIP UA. Once the two SIP UA parties are successfully connected, the device requests the PBX to disconnect the ISDN call, thereby freeing resources on the PBX.

For example, assume legacy PBX user "A" has two established calls connected through the device – one with remote SIP UA "B" and the other with SIP UA "C". In this scenario, user "A" initiates a consultation call transfer to connect "B" with "C". The device receives the consultation call transfer request from the PBX and then connects "B" with "C", by sending "B" a REFER message with a Replaces header (i.e., replace caller "A" with "C"). Upon receipt of a SIP NOTIFY 200 message in response to the REFER, the device sends a Q.931 Disconnect messages to the PBX, notifying the PBX that it can disconnect the ISDN calls (of user "A").

This feature is enabled by the QSIGPathReplacementMode parameter.

### 30.5.3 Blind Call Transfer

Blind call transfer is done (using SIP REFER messages) after a call is established between call parties A and B, and party A decides to immediately transfer the call to C without first speaking to C. The result of the transfer is a call between B and C (similar to consultation transfer, but skipping the consultation stage).

You can also use the ManipulateIP2PSTNReferTo parameter to manipulate the destination number according to the number received in the SIP Refer-To header. This is applicable to all types of blind transfers to the PSTN (e.g., TBCT, ECT, RLT, QSIG, FXO, and CAS). During blind transfer, the device initiates a new call to the PSTN and the destination number of this call can be manipulated if this parameter is enabled. The following is an example of such a blind transfer:

1. IP phone "A" calls PSTN phone "B", and the call is established.
2. "A" performs a blind transfer to PSTN phone "C". It does this as follows:
  - a. "A" sends a SIP REFER message (with the phone number of "C" in the Refer-To header) to the device.

- b. The device sends a Q.931 Setup message to "C". This feature enables manipulating the called party number in this outgoing Setup message.

The manipulation is done as follows:

1. If you configure a value for the xferPrefix parameter, then this value (string) is added as a prefix to the number in the Refer-To header.
2. This called party number is then manipulated using the IP-to-Tel Destination Phone Number Manipulation table.
3. The source number of the transferred call is taken from the original call, according to its initial direction:
  - Tel-to-IP call: source number of the original call.
  - IP-to-Tel call: destination number of the original call.
  - If the UseReferredByForCallingNumber parameter is set to 1, the source number is taken from the SIP Referred-By header if included in the received SIP REFER message.

This source number can also be used as the value for the 'Source Prefix' field in the IP-to-Tel Destination Phone Number Manipulation table. The local IP address is used as the value for the 'Source IP Address' field.



**Note:** Manipulation using the ManipulateIP2PSTNReferTo parameter does not affect IP-to-Trunk Group routing rules.

## 30.6 Call Forward

For digital interfaces: The device supports Call Deflection (ETS-300-207-1) for Euro ISDN and QSIG (ETSI TS 102 393) for Network and User sides, which provides IP-ISDN interworking of call forwarding (call diversion) when the device receives a SIP 302 response.

Call forward performed by the SIP side: Upon receipt of a Facility message with Call Rerouting IE from the PSTN, the device initiates a SIP transfer process by sending a SIP 302 (including the Call Rerouting destination number) to the IP in response to the remote SIP entity's INVITE message. The device then responds with a Disconnect message to the PSTN side.

Call forward performed by the PSTN side: When the device sends the INVITE message to the remote SIP entity and receives a SIP 302 response, the device sends a Facility message with the same IE mentioned above to the PSTN, and waits for the PSTN side to disconnect the call. This is configured using the CallReroutingMode.

For analog interfaces: The following methods of call forwarding are supported:

- Immediate: incoming call is forwarded immediately and unconditionally.
- Busy: incoming call is forwarded if the endpoint is busy.
- No Reply: incoming call is forwarded if it isn't answered for a specified time.
- On Busy or No Reply: incoming call is forwarded if the port is busy or when calls are not answered after a specified time.
- Do Not Disturb: immediately reject incoming calls. Upon receiving a call for a Do Not Disturb, the 603 Decline SIP response code is sent.

Three forms of forwarding parties are available:

- Served party: party configured to forward the call (FXS device).
- Originating party: party that initiates the first call (FXS or FXO device).
- Diverted party: new destination of the forwarded call (FXS or FXO device).

The served party (FXS interface) can be configured through the Web interface (see Configuring Call Forward on page 399) or ini file to activate one of the call forward modes. These modes are configurable per endpoint.



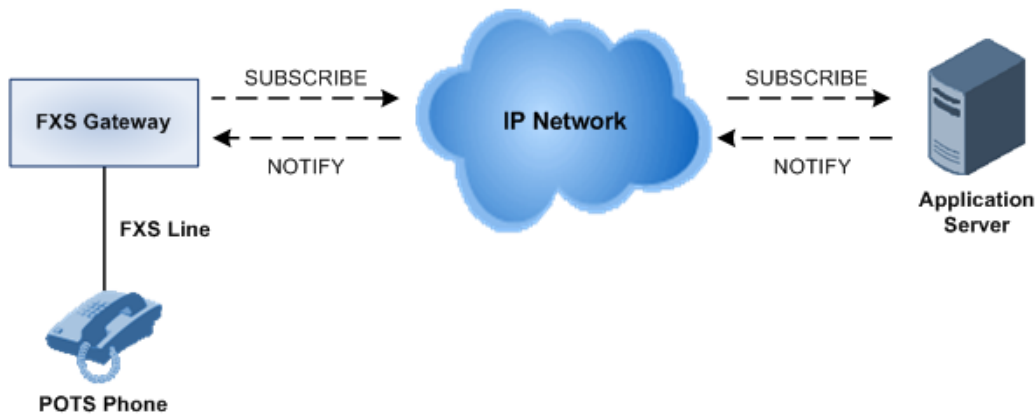
**Notes:**

- When call forward is initiated, the device sends a SIP 302 response with a contact that contains the phone number from the forward table and its corresponding IP address from the routing table (or when a proxy is used, the proxy's IP address).
- For receiving call forward, the device handles SIP 3xx responses for redirecting calls with a new contact.

### 30.6.1 Call Forward Reminder Ring

The device supports the Call Forward Reminder Ring feature for FXS interfaces, whereby the device's FXS endpoint emits a short ring burst, only in **onhook** state, when a third-party Application Server (e.g., softswitch) forwards an incoming call to another destination. This is important in that it notifies (audibly) the FXS endpoint user that a call forwarding service is currently being performed.

**Figure 30-3: Call Forward Reminder with Application Server**



The device generates a Call Forward Reminder ring burst to the FXS endpoint each time it receives a SIP NOTIFY message with a "reminder ring" xml body. The NOTIFY request is sent from the Application Server to the device each time the Application Server forwards an incoming call. The service is cancelled when an UNSUBSCRIBE request is sent from the device, or when the Subscription time expires.

The reminder-ring tone can be defined by using the parameter `CallForwardRingToneID`, which points to a ring tone defined in the Call Progress Tone file.

The following parameters are used to configure this feature:

- `EnableNRTSubscription`
- `ASSubscribeIPGroupID`
- `NRTSubscribeRetryTime`
- `CallForwardRingToneID`

### 30.6.2 Call Forward Reminder (Off-Hook) Special Dial Tone

The device plays a special dial tone (stutter dial tone - Tone Type #15) to a specific FXS endpoint when the phone is off-hooked and when a third-party Application server (AS),



e.g., a softswitch is used to forward calls intended for the endpoint, to another destination. This is useful in that it reminds the FXS user of this service. This feature does not involve device subscription (SIP SUBSCRIBE) to the AS.

Activation/deactivation of the service is notified by the server. An unsolicited SIP NOTIFY request is sent from the AS to the device when the Call Forward service is activated or deactivated. Depending on this NOTIFY request, the device plays either the standard dial tone or the special dial tone for Call Forward.

For playing the special dial tone, the received SIP NOTIFY message must contain the following headers:

- **From and To:** contain the same information, indicating the specific endpoint
- **Event:** ua-profile
- **Content-Type:** "application/simserv+xml"
- Message body is the XML body and contains the "dial-tone-pattern" set to "special-condition-tone" (<ss:dial-tone-pattern>special-condition-tone</ss:dial-tone-pattern>), which is the special tone indication.

To cancel the special dial tone and playing the regular dial tone, the received SIP NOTIFY message must contain the following headers:

- **From and To:** contain the same information, indicating the specific endpoint
- **Event:** ua-profile
- **Content-Type:** "application/simserv+xml"
- Message body is the XML body containing the "dial-tone-pattern" set to "standard-condition-tone" (<ss:dial-tone-pattern>standard-condition-tone</ss:dial-tone-pattern>), which is the regular dial tone indication.

Therefore, the special dial tone is valid until another SIP NOTIFY is received that instructs otherwise (as described above).



**Note:** if the MWI service is active, the MWI dial tone overrides this special Call Forward dial tone.

### 30.6.3 Call Forward Reminder Dial Tone (Off-Hook) upon Spanish SIP Alert-Info

The device plays a special dial tone to FXS phones in off-hook state that are activated with the call forwarding service. The special dial tone is used as a result of the device receiving a SIP NOTIFY message from a third-party softswitch providing the call forwarding service with the following SIP Alert-Info header:

```
Alert-Info: <http://127.0.0.1/Tono-Espec-Invitacion>;lpi-aviso=Desvio-Inmediato
```

This special tone is a stutter dial tone (Tone Type = 15), as defined in the CPT file.

The FXS phone user, connected to the device, activates the call forwarding service by dialing a special number (e.g., \*21\*xxxx) and as a result, the device sends a regular SIP INVITE message to the softswitch. The softswitch later notifies of the activation of the forwarding service by sending an unsolicited NOTIFY message with the Alert-Info header, as mentioned above.

When the call forwarding service is de-activated, for example, by dialing #21# and sending an INVITE with this number, the softswitch sends another SIP NOTIFY message with the following Alert-Info header:

```
Alert-Info: <http://127.0.0.1/ Tono-Normal-Invitacion>; Aviso = Desvió-Inmediato
```

From this point on, the device plays a normal dial tone to the FXS phone when it goes off-hook.



### 30.6.4 BRI Call Forwarding

The device supports call forwarding (CF) services initiated by ISDN Basic BRI phones connected to it. Upon receipt of an ISDN Facility message for call forward from the BRI phone, the device sends a SIP INVITE to the softswitch with a user-defined code in the SIP To header, representing the reason for the call forward.

The codes for the call forward can be defined using the following parameters:

- SuppServCodeCFU - Call Forward Unconditional
- SuppServCodeCFUDeact - Call Forward Unconditional Deactivation
- SuppServCodeCFB - Call Forward on Busy
- SuppServCodeCFBDeact - Call Forward on Busy Deactivation
- SuppServCodeCFNR - Call Forward on No Reply
- SuppServCodeCFNRDeact - Call Forward on No Reply Deactivation



**Note:** These codes must be defined according to the settings of the softswitch (i.e., the softswitch must recognize them).

Below is an example of an INVITE message sent by the device indicating an unconditional call forward ("\*72") to extension number 100. This code is defined using the SuppServCodeCFU parameter.

```
INVITE sip:*72100@10.33.8.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.5:5060;branch=z9hG4bKWDSUKUHWFEQSVUUVJGM
From: <sip:400@10.33.2.5;user=phone>;tag=DUOROSXSJOYJLNBFRQTG
To: <sip:*72100@10.33.8.53;user=phone>
Call-ID: GMNOVQRRXUUCYCQSFQHS@10.33.2.5
CSeq: 1 INVITE
Contact: <sip:400@10.33.2.5:5060>
Supported: em,100rel,timer,replaces
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE
User-Agent: Sip Message Generator V1.0.0.5
User-to-User: 31323334;pd=4
Content-Type: application/sdp
Content-Length: 155
```

## 30.7 Call Waiting

The Call Waiting feature enables FXS devices to accept an additional (second) call on busy endpoints. If an incoming IP call is designated to a busy port, the called party hears a call waiting tone (several configurable short beeps) and (for Bellcore and ETSI Caller IDs) can view the Caller ID string of the incoming call. The calling party hears a call waiting ringback tone. The called party can accept the new call using hook-flash, and can toggle between the two calls.

#### ➤ To enable call waiting:

1. Set the parameter EnableCallWaiting to 1.
2. Set the parameter EnableHold to 1.
3. Define the Call Waiting indication and call waiting ringback tones in the Call Progress Tones file. You can define up to four call waiting indication tones (refer to the

FirstCallWaitingToneID parameter).

4. To configure the call waiting indication tone cadence, modify the following parameters: NumberOfWaitingIndications, WaitingBeepDuration and TimeBetweenWaitingIndications.
5. To configure a delay interval before a Call Waiting Indication is played to the currently busy port, use the parameter TimeBeforeWaitingIndication. This enables the caller to hang up before disturbing the called party with Call Waiting Indications. Applicable only to FXS modules.

Both the calling and called sides are supported by FXS interfaces; FXO interfaces support only the calling side.

To indicate Call Waiting, the device sends a 182 Call Queued response. The device identifies Call Waiting when a 182 Call Queued response is received.



**Note:** The Call Waiting feature is applicable only to FXS/FXO interfaces.

## 30.8 Message Waiting Indication

The device supports Message Waiting Indication (MWI) according to IETF RFC 3842, including SUBSCRIBE to an MWI server.

For analog interfaces: The FXS device can accept an MWI NOTIFY message that indicates waiting messages or that the MWI is cleared. Users are informed of these messages by a stutter dial tone. The stutter and confirmation tones are defined in the CPT file. If the MWI display is configured, the number of waiting messages is also displayed. If the MWI lamp is configured, the phone's lamp (on a phone that is equipped with an MWI lamp) is lit. The device can subscribe to the MWI server per port (usually used on FXS) or per device (used on FXO).



**Notes:**

- For more information on IP voice mail configuration, refer to the *IP Voice Mail CPE Configuration Guide*.
- For creating a CPT file using AudioCodes CPTWizard utility, refer to CPTWizard Utility User's Guide.

To configure MWI, use the following parameters:

- EnableMWI
- MWIServerIP, or MWISubscribeIPGroupID and ProxySet
- MWIAnalogLamp
- MWIDisplay
- StutterToneDuration
- EnableMWISubscription
- MWIExpirationTime
- SubscribeRetryTime
- SubscriptionMode
- CallerIDType (determines the standard for detection of MWI signals)
- ETSIVMWITypeOneStandard
- BellcoreVMWITypeOneStandard

- VoiceMailInterface
- EnableVMURI

The device supports the following MWI features for its digital PSTN interfaces:

- For BRI interfaces: This feature provides support for MWI on BRI phones connected to the device and using the Euro ISDN BRI variant. When this feature is activated and a voice mail message is recorded to the mail box of a BRI extension, the softswitch sends a notification to the device. In turn, the device notifies the BRI extension and a red light flashes on the BRI extension's phone. Once the voice message is retrieved, the MWI light on the BRI extension turns off. This feature is configured by setting the VoiceMailInterface parameter to 8 ("ETSI") and enabled by the EnableMWI parameter.
- Euro-ISDN MWI: The device supports Euro-ISDN MWI for IP-to-Tel calls. The device interworks SIP MWI NOTIFY messages to Euro-ISDN Facility information element (IE) MWI messages. This is supported by setting the VoiceMailInterface parameter to 8.
- QSIG MWI: The device also supports the interworking of QSIG MWI to IP (in addition to interworking of SIP MWI NOTIFY to QSIG Facility MWI messages). This provides interworking between an ISDN PBX with voicemail capabilities and a softswitch, which requires information on the number of messages waiting for a specific user. This support is configured using the TrunkGroupSettings\_MWInterrogationType parameter (in the Trunk Group Settings table), which determines the device's handling of MWI Interrogation messages. The process for sending the MWI status upon request from a softswitch is as follows:

12. The softswitch sends a SIP SUBSCRIBE message to the device.
13. The device responds by sending an empty SIP NOTIFY to the softswitch, and then sending an ISDN Setup message with Facility IE containing an MWI Interrogation request to the PBX.
14. The PBX responds by sending to the device an ISDN Connect message containing Facility IE with an MWI Interrogation result, which includes the number of voice messages waiting for the specific user.
15. The device sends another SIP NOTIFY to the softswitch, containing this MWI information.
16. The SIP NOTIFY messages are sent to the IP Group defined by the NotificationIPGroupID parameter.

In addition, when a change in the status occurs (e.g., a new voice message is waiting or the user has retrieved a message from the voice mail), the PBX initiates an ISDN Setup message with Facility IE containing an MWI Activate request, which includes the new number of voice messages waiting for the user. The device forwards this information to the softswitch by sending a SIP NOTIFY.

Depending on the PBX support, the MWInterrogationType parameter can be configured to handle these MWI Interrogation messages in different ways. For example, some PBXs support only the MWI Activate request (and not MWI Interrogation request). Some support both these requests. Therefore, the device can be configured to disable this feature, or enable it with one of the following support:

- Responds to MWI Activate requests from the PBX by sending SIP NOTIFY MWI messages (i.e., does not send MWI Interrogation messages).
- Send MWI Interrogation message, but don't use its result. Instead, wait for MWI Activate requests from the PBX.
- Send MWI Interrogation message, use its result, and use the MWI Activate requests.

## 30.9 Caller ID

This section describes the device's Caller ID support.



**Note:** The Caller ID feature is applicable only to FXS/FXO interfaces.

### 30.9.1 Caller ID Detection / Generation on the Tel Side

By default, generation and detection of Caller ID to the Tel side is disabled. To enable Caller ID, set the parameter EnableCallerID to 1. When the Caller ID service is enabled:

- For FXS: the Caller ID signal is sent to the device's port
- For FXO: the Caller ID signal is detected

The configuration for Caller ID is described below:

- Use the parameter CallerIDType to define the Caller ID standard. Note that the Caller ID standard that is used on the PBX or phone must match the standard defined in the device.
- Select the Bellcore caller ID sub standard using the parameter BellcoreCallerIDTypeOneSubStandard
- Select the ETSI FSK caller ID sub standard using the parameter ETSICallerIDTypeOneSubStandard
- Enable or disable (per port) the caller ID generation (for FXS) and detection (for FXO) using the 'Generate / Detect Caller ID to Tel' table (EnableCallerID). If a port isn't configured, its caller ID generation / detection are determined according to the global parameter EnableCallerID.
- EnableCallerIDTypeTwo: disables / enables the generation of Caller ID type 2 when the phone is off-hooked (used for call waiting).
- RingsBeforeCallerID: sets the number of rings before the device starts detection of caller ID (FXO only). By default, the device detects the caller ID signal between the first and second rings.
- AnalogCallerIDTimingMode: determines the time period when a caller ID signal is generated (FXS only). By default, the caller ID is generated between the first two rings.
- PolarityReversalType: some Caller ID signals use reversal polarity and/or wink signals. In these scenarios, it is recommended to set PolarityReversalType to 1 (Hard) (FXS only).
- The Caller ID interworking can be changed using the parameters UseSourceNumberAsDisplayName and UseDisplayNameAsSourceNumber.

### 30.9.2 Debugging a Caller ID Detection on FXO

The procedure below describes debugging caller ID detection in FXO interfaces.

➤ **To debug a Caller ID detection on an FXO interface:**

1. Verify that the parameter EnableCallerID is set to 1.
2. Verify that the caller ID standard (and substandard) of the device matches the standard of the PBX (using the parameters CallerIDType, BellcoreCallerIDTypeOneSubStandard, and ETSICallerIDTypeOneSubStandard).

3. Define the number of rings before the device starts the detection of caller ID (using the parameter `RingsBeforeCallerID`).
4. Verify that the correct FXO coefficient type is selected (using the parameter `CountryCoefficients`), as the device is unable to recognize caller ID signals that are distorted.
5. Connect a phone to the analog line of the PBX (instead of to the device's FXO interface) and verify that it displays the caller ID.

If the above does not solve the problem, you need to record the caller ID signal (and send it to `AudioCodes`), as described below.

➤ **To record the caller ID signal using the debug recording mechanism:**

1. Access the FAE page (by appending "FAE" to the device's IP address in the Web browser's URL, for example, `http://10.13.4.13/FAE`).
2. Press the **Cmd Shell** link.
3. Enter the following commands:

```
dr
ait <IP address of PC to collect the debug traces sent from
the device>
AddChannelIdTrace ALL-WITH-PCM <port number, which starts from
0>
Start
```

4. Make a call to the FXO.
5. To stop the DR recording, at the CLI prompt, type **STOP**.

### 30.9.3 Caller ID on the IP Side

Caller ID is provided by the SIP From header containing the caller's name and "number", for example:

```
From: "John" <SIP:101@10.33.2.2>;tag=35dfsgasd45dg
```

If Caller ID is restricted (received from Tel or configured in the device), the From header is set to:

```
From: "anonymous" <anonymous@anonymous.invalid>; tag=35dfsgasd45dg
```

The P-Asserted (or P-Preferred) headers are used to present the originating party's caller ID even when the caller ID is restricted. These headers are used together with the Privacy header.

- If Caller ID is restricted:
  - The From header is set to "anonymous" <anonymous@anonymous.invalid>
  - The 'Privacy: id' header is included
  - The P-Asserted-Identity (or P-Preferred-Identity) header shows the caller ID
- If Caller ID is allowed:
  - The From header shows the caller ID
  - The 'Privacy: none' header is included
  - The P-Asserted-Identity (or P-Preferred-Identity) header shows the caller ID

The caller ID (and presentation) can also be displayed in the Calling Remote-Party-ID header.

The 'Caller Display Information' table (`CallerDisplayInfo`) is used for the following:

- **FXS interfaces** - to define the caller ID (per port) that is sent to IP.
- **FXO interfaces** - to define the caller ID (per port) that is sent to IP if caller ID isn't detected on the Tel side, or when `EnableCallerID = 0`.

- **FXS and FXO interfaces** - to determine the presentation of the caller ID (allowed or restricted).
- **To maintain backward compatibility** - when the strings 'Private' or 'Anonymous' are set in the Caller ID/Name field, the caller ID is restricted and the value in the Presentation field is ignored.

The value of the 'Presentation' field that is defined in the 'Caller Display Information' table can be overridden by configuring the 'Presentation' parameter in the 'Tel to IP Source Number Manipulation' table. Therefore, this table can be used to set the presentation for specific calls according to Source / Destination prefixes.

The caller ID can be restricted/allowed (per port) using keypad features KeyCLIR and KeyCLIRDeact (FXS only).

AssertedIdMode defines the header that is used (in the generated INVITE request) to deliver the caller ID (P-Asserted-Identity or P-Preferred-Identity). Use the parameter UseTelURIForAssertedID to determine the format of the URI in these headers (sip: or tel:).

The parameter EnableRPIheader enables Remote-Party-ID (RPI) headers for calling and called numbers for Tel-to-IP calls.

## 30.10 Three-Way Conferencing

The device supports three-way conference calls. These conference calls can also occur simultaneously. The device supports the following conference modes (configured by the parameter 3WayConferenceMode):

- **Conferencing managed by an external, AudioCodes Conference (media) server:**  
The Conference-initiating INVITE sent by the device uses the ConferenceID concatenated with a unique identifier as the Request-URI. This same Request-URI is set as the Refer-To header value in the REFER messages that are sent to the two remote parties. For this mode, the 3WayConferenceMode parameter is set to 0 (default.)
- **Conferencing managed by an external, third-party Conference (media) server:**  
The Conference-initiating INVITE sent by the device uses only the ConferenceID as the Request-URI. The Conference server sets the Contact header of the 200 OK response to the actual unique identifier (Conference URI) to be used by the participants. This Conference URI is included (by the device) in the Refer-To header value in the REFER messages sent by the device to the remote parties. The remote parties join the conference by sending INVITE messages to the Conference server using this conference URI. For this mode, the 3WayConferenceMode parameter is set to 1.
- **Local, on-board conferencing:** The conference is established on the device without the need for an external Conference server. This feature includes local mixing and transcoding of the 3-Way Call legs on the device, and even allowing multi-codec conference calls. The number of simultaneous, on-board conferences can be limited using the parameter MaxInBoardConferenceCalls. The device supports up to five simultaneous, on-board, three-way conference calls. For this mode, the 3WayConferenceMode parameter is set to 2.

**Notes:**

- Three-way conferencing using an external conference server is supported only by FXS interfaces.
- Instead of using the flash-hook button to establish a three-way conference call, you can dial a user-defined hook-flash code (e.g., "\*1"), configured by the HookFlashCode parameter.
- Three-way conferencing is applicable only to FXS and BRI interfaces. Three-way conferencing support for the BRI phones connected to the device complies with ETS 300 185.
- The device supports high definition, three-way conferencing using wideband codecs (e.g., G.722 and AMR-WB). This allows conference participants to experience wideband voice quality. Call conferences can also include narrowband and wideband participants.

The following example demonstrates three-way conferencing using the device's local, on-board conferencing feature. In this example, telephone "A" connected to the device establishes a three-way conference call with two remote IP phones, "B" and "C":

1. A establishes a regular call with B.
2. A places B on hold, by pressing the telephone's flash-hook button.
3. A hears a dial tone and then makes a call to C.
4. C answers the call.
5. A establishes a three-way conference call with B and C, by pressing the flash-hook button and digit 3.

To configure this local, on-board three-way conferencing:

6. Open the Supplementary Services page.
7. Set 'Enable 3-Way Conference' to **Enable** (Enable3WayConference = 1).
8. Set 'Three Way Conference Mode' to **On Board** (3WayConferenceMode = 2).
9. Set 'Flash Keys Sequence Style' to **Sequence 1** or **Sequence 2** (FlashKeysSequenceStyle = 1 or 2).

## 30.11 Emergency E911 Phone Number Services

This section describes the device's support for emergency phone number services. The device supports the North American emergency telephone number system known as Enhanced 911 (E911), according to the TR-TSY-000350 and Bellcore's GR-350-Jun2003 standards. The E911 emergency system automatically associates a physical address with the calling party's telephone number, and routes the call to the most appropriate (closest) Public Safety Answering Point (PSAP), allowing the PSAP to quickly dispatch emergency response (e.g., police) to the caller's location.

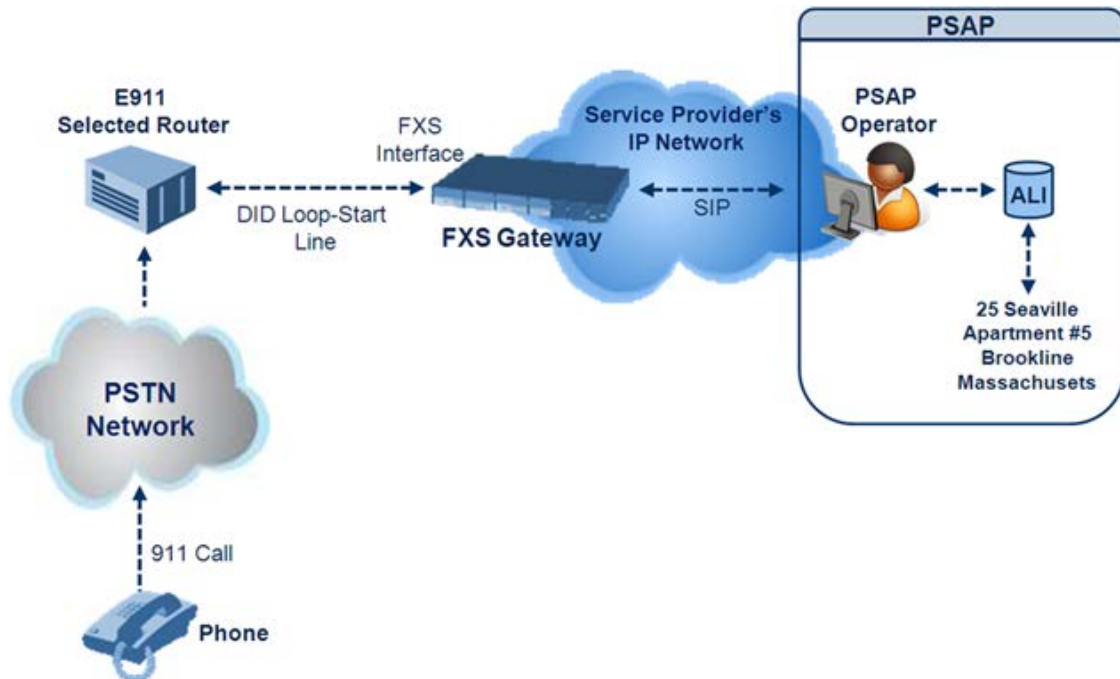
Typically, the dialed emergency number is routed to the appropriate PSAP by the telephone company's switch, known as a 911 Selective Router (or E911 tandem switch). If the PSAP receives calls from the telephone company on old-style digital trunks, they are specially formatted Multi-Frequency (MF) trunks that pass only the calling party's number (known as Automatic Number Identification - ANI). Once the PSAP receives the call, it searches for the physical address that is associated with the calling party's telephone number (in the Automatic Location Identification database - ALI).



### 30.11.1 FXS Device Emulating PSAP using DID Loop-Start Lines

The device's FXS interface can be configured to emulate PSAP (using DID loop start lines), according to the Telcordia GR-350-CORE specification.

**Figure 30-4: FXS Device Emulating PSAP using DID Loop-Start Lines**



The call flow of an E911 call to the PSAP is as follows:

1. The E911 tandem switch seizes the line.
2. The FXS device detects the line seize, and then generates a wink signal (nominal 250 msec). The wink can be delayed by configuring the parameter DelayBeforeDIDWink to 200 (for 200 msec or a higher value).
3. The switch detects the wink and then sends the MF Spill digits with ANI and (optional) Pseudo-ANI (P ANI).
4. The FXS device collects the MF digits, and then sends a SIP INVITE message to the PSAP with all collected MF digits in the SIP From header as one string.
5. The FXS device generates a mid-call wink signal (two subsequent polarity reversals) toward the E911 tandem switch upon either detection of an RFC 2833 "hookflash" telephony event, or if a SIP INFO message with a "hooflash" body is received from the PSAP (see the example below). The duration of this "flashhook" wink signal is configured using the parameter FlashHookPeriod (usually 500 msec). Usually the wink signal is followed by DTMF digits sent by PSAP to perform call transfer. Another way to perform the call transfer is to use SIP REFER messages, as described below.
6. The FXS device supports call transfer initiated by the PSAP. If it receives a SIP REFER message with the Refer-To URI host part containing an IP address that is equal to the device's IP address, the FXS device generates a 500-msec wink signal (double polarity reversals), and then (after a user-defined interval configured by the parameter WaitForDialTime), plays DTMF digits according to the transfer number received in the SIP Refer-To header URI userpart.
7. When the call is answered by the PSAP operator, the PSAP sends a SIP 200 OK to the FXS device, and the FXS device then generates a polarity reversal signal to the E911 switch.
8. After the call is disconnected by the PSAP, the PSAP sends a SIP BYE to the FXS device, and the FXS device reverses the polarity of the line toward the tandem switch.



The following parameters need to be configured:

- EnableDIDWink = 1
- EnableReversalPolarity = 1
- PolarityReversalType = 1
- FlashHookPeriod = 500 (for 500 msec "hookflash" mid-call Wink)
- WinkTime = 250 (for 250 msec signalling Wink generated by the FXS device after it detects the line seizure)
- EnableTransfer = 1 (for call transfer)
- LineTransferMode = 1 (for call transfer)
- WaitforDialTime = 1000 (for call transfer)
- SwapTEI2IPCalled&CallingNumbers = 1
- DTMFDetectorEnable = 0
- MFR1DetectorEnable = 1
- DelayBeforeDIDWink = 200 (for 200 msec) - can be configured in the range from 0 (default) to 1000.



**Note:** Modification of the WinkTime and FlashHookPeriod parameters require a device reset.

The outgoing SIP INVITE message contains the following headers:

```
INVITE sip:Line@DomainName
From: <sip:*81977820#@sipgw>;tag=1c143
To: <sip:Line@DomainName>
```

Where:

- *Line* = as configured in the Endpoint Phone Number Table
- *SipGtw* = configured by the SIPGatewayName parameter
- *From* header/user part = calling party number as received from the MF spill

The ANI and the pseudo-ANI numbers are sent to the PSAP either in the From and/or P-AssertedID SIP header.

Typically, the MF spills are sent from the E911 tandem switch to the PSAP, as shown in the table below:

**Dialed MF Digits Sent to PSAP**

Digits of Calling Number	Dialed MF Digits
8 digits "nnnnnnnn" (ANI)	"KPnnnnnnnnST"
12 digits "nnnnnnnnnnnn" (ANI)	"KPnnnnnnnnnnnnSTP"
12 digits ANI and 10 digits PANI	"KPnnnnnnnnnnnnSTKPmmmmmmmmmmST"
two digits "nn"	"KPnnSTP"

The MF KP, ST, and STP digits are mapped as follows:

- \* for KP
- # for ST
- B for STP

For example, if ANI and PANI are received, the SIP INVITE contains the following From header:

```
From: <sip:nnnnnnnnnnnnn#*nnnnnnnnnnnn#@10.2.3.4>;tag=1c14
```



**Note:** It is possible to remove the \* and # characters, using the device's number manipulation rules.

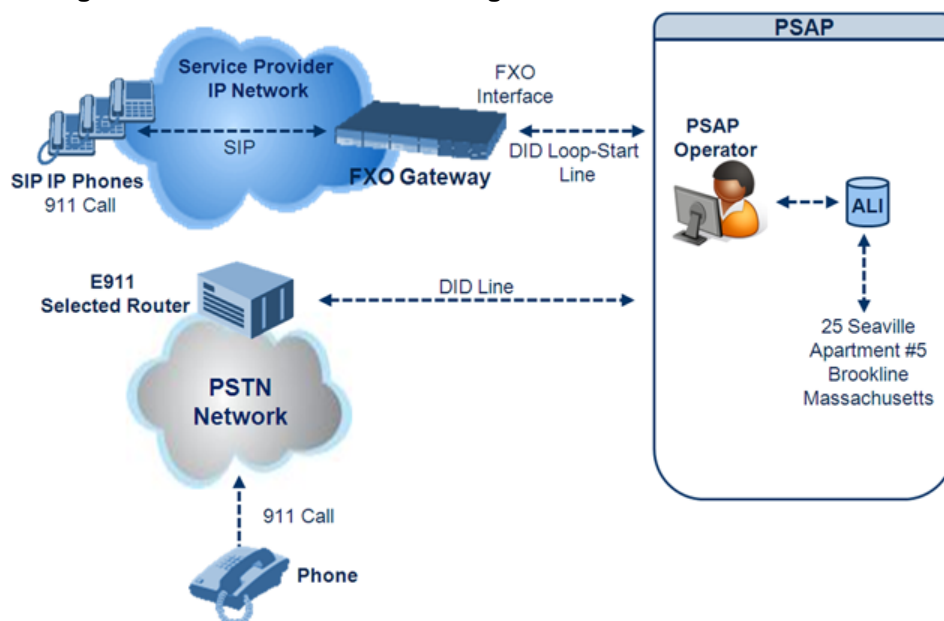
If the device receives the SIP INFO message below, it then generates a "hookflash" mid-call Wink signal:

```
INFO sip:4505656002@192.168.13.40:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.13.2:5060
From: portlvegal <sip:06@192.168.13.2:5060>
To: <sip:4505656002@192.168.13.40:5060>;tag=132878796-1040067870294
Call-ID: 0010-0016-D69A7DA8-1@192.168.13.2
CSeq:2 INFO
Content-Type: application/broadsoft
Content-Length: 17
event flashhook
```

### 30.11.2 FXO Device Interworking SIP E911 Calls from Service Provider's IP Network to PSAP DID Lines

The device's FXO interface can interwork SIP emergency E911 calls from the Service Provider's IP network to the analog PSAP DID lines. The standards that define this interface include TR-TSY-000350 or Bellcore's GR-350-Jun2003. This protocol defines signaling between the E911 tandem switch (E911 Selective Router) and the PSAP, using analog loop-start lines. The FXO device can be implemented instead of an E911 switch, by connecting directly to the PSAP DID loop-start lines.

**Figure 30-5: FXO Device Interfacing between E911 Switch and PSAP**



When an IP phone subscriber dials 911, the device receives the SIP INVITE message and makes a call to the PSAP as follows:

1. The FXO device seizes the line.
2. PSAP sends a Wink signal (250 msec) to the device.
3. Upon receipt of the Wink signal, the device dials MF digits after a user-defined time (WaitForDialTime) containing the caller's ID (ANI) obtained from the SIP headers From or P-Asserted-Identity.
4. When the PSAP operator answers the call, the PSAP sends a polarity reversal to the device, and the device then sends a SIP 200 OK to the IP side.
5. After the PSAP operator disconnects the call, the PSAP reverses the polarity of the line, causing the device to send a SIP BYE to the IP side.
6. If, during active call state, the device receives a Wink signal (typically of 500 msec) from the PSAP, the device generates a SIP INFO message that includes a "hookflash" body, or sends RFC 2833 hookflash Telephony event (according to the HookFlashOption parameter).
7. Following the "hookflash" Wink signal, the PSAP sends DTMF digits. These digits are detected by the device and forwarded to the IP, using RFC 2833 telephony events (or inband, depending on the device's configuration). Typically, this Wink signal followed by the DTMF digits initiates a call transfer.

For supporting the E911 service, used the following configuration parameter settings:

- Enable911PSAP = 1 (also forces the EnableDIDWink and EnableReversalPolarity)
- HookFlashOption = 1 (generates the SIP INFO hookflash message) or 4 for RFC 2833 telephony event
- WinkTime = 700 (defines detection window of 50 to 750 msec for detection of both winks - 250 msec wink sent by the PSAP for starting the device's dialing; 500 msec wink during the call)
- IsTwoStageDial = 0
- EnableHold = 0
- EnableTransfer = 0
  - Use RFC 2833 DTMF relay:
    - ◆ RxDTMFOption = 3
    - ◆ TxDTMFOption = 4
    - ◆ RFC2833PayloadType = 101
- TimeToSampleAnalogLineVoltage = 100
- WaitForDialTime = 1000 (default is 1 sec)
- SetDefaultLinePolarityState = 0 (you need to verify that the RJ-11 two-wire cable is connected without crossing, Tip to Tip, Ring to Ring. Typically, the Tip line is positive compared to the Ring line.)



**Note:** If the two-wire cable is crossed, the SetDefaultLinePolarityState parameter must be set to 1.

The device expects to receive the ANI number in the From and/or P-Asserted-Identity SIP header. If the pseudo-ANI number exists, it should be sent as the display name in these headers.

Dialed Number by Device Depending on Calling Number

Digits of Calling Number (ANI)	Digits of Displayed Number	Number Dialed MF Digits
8 "nnnnnnnn"	-	MF dialed "KPnnnnnnnnST"
12 "nnnnnnnnnnnn"	None	"KPnnnnnnnnnnnnSTP"
12 "nnnnnnnnnnnn"	10 "mmmmmmmmmm" (pANI)	"KPnnnnnnnnnnnnSTKPmmmmmmmmmmS T"
2 "nn"	None	"KPnnSTP"
1 "n"	-	MF dialed "KPnST"  For example: "From: <sip:8>@xyz.com>" generates device MF spill of KP 8 ST

Table notes:

- For all other cases, a SIP 484 response is sent.
- KP is for .
- ST is for #.
- STP is for B.

The MF duration of all digits, except for the KP digit is 60 msec. The MF duration of the KP digit is 120 msec. The gap duration is 60 msec between any two MF digits.



#### Notes:

- Manipulation rules can be configured for the calling (ANI) and called number (but not on the "display" string), for example, to strip 00 from the ANI "00INXXXXYY".
- The called number, received as userpart of the Request URI ("301" in the example below), can be used to route incoming SIP calls to FXO specific ports, using the TrunkGroup and PSTNPrefix parameters.
- When the PSAP party off-hooks and then immediately on-hooks (i.e., the device detects wink), the device releases the call sending SIP response "403 Forbidden" and the release reason 21 (i.e., call rejected) "Reason: Q.850 ;cause=21" is sent. Using the cause mapping parameter, it is possible to change the 403 to any other SIP reason, for example, to 603.
- Sometimes a wink signal sent immediately after the FXO device seizes the line is not detected. To overcome this problem, configure the parameter TimeToSampleAnalogLineVoltage to 100 (instead of 1000 msec, which is the default value). The wink is then detected only after this timeout + 50 msec (minimum 150 msec).

Below are two examples for a) INVITE messages and b) INFO messages generated by hook-flash.

- **Example A:** INVITE message with ANI = 333333444444 and pseudo-ANI = 0123456789:

```
INVITE sip:301@10.33.37.79;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac771627168
Max-Forwards: 70
```

```

From: "0123456789"
<sip:33333344444@audiocodes.com>;tag=1c771623824
To: <sip:301@10.33.37.79;user=phone>
Call-ID: 77162335841200014153@10.33.37.78
CSeq: 1 INVITE
Contact: <sip:101@10.33.37.78>
Supported: em,100rel,timer,replaces,path
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO
,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-FXO/v.6.00A.020.077
Privacy: none
P-Asserted-Identity: "0123456789"
<sip:33333344444@audiocodes.com>
Content-Type: application/sdp
Content-Length: 253
v=0
o=AudiocodesGW 771609035 771608915 IN IP4 10.33.37.78
s=Phone-Call
c=IN IP4 10.33.37.78
t=0 0
m=audio 4000 RTP/AVP 8 0 101
a=rtpmap:8 pcma/8000
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv

```

- **Example B:** The detection of a Wink signal generates the following SIP INFO message:

```

INFO sip:4505656002@192.168.13.40:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.13.2:5060
From: portlvegal <sip:06@192.168.13.2:5060>
To: <sip:4505656002@192.168.13.40:5060>;tag=132878796-
1040067870294
Call-ID: 0010-0016-D69A7DA8-1@192.168.13.2
CSeq:2 INFO
Content-Type: application/broadsoft
Content-Length: 17
event flashhook

```

### 30.11.3 Pre-empting Existing Calls for E911 IP-to-Tel Calls

If the device receives an E911 call from the IP network destined to the Tel, and there are unavailable channels (e.g., all busy), the device terminates one of the calls (arbitrary) and then sends the E911 call to that channel. The preemption is done only on a channel pertaining to the same Trunk Group for which the E911 call was initially destined and if the channel select mode (configured by the ChannelSelectMode parameter) is set to a value other than "By Dest Number" (0).

The preemption is done only if the incoming IP-to-Tel call is identified as an emergency call. The device identifies emergency calls by one of the following:

- The destination number of the IP call matches one of the numbers defined by the EmergencyNumbers parameter. For E911, you must defined this parameter with the value "911".
- The Priority header of the incoming SIP INVITE message contains the "emergency" value.

Emergency pre-emption of calls can be enabled for all calls, using the global parameter `CallPriorityMode`, or for specific calls using the Tel Profile parameter `CallPriorityMode`.



**Notes:**

- For Trunk Groups configured with call preemption, all must be configured to MLPP [1] or all configured to Emergency [2]. In other words, you cannot set some trunks to [1] and some to [2].
- The global parameter must be set to the same value as that of the Tel Profile parameter; otherwise, the Tel Profile parameter is not applied.
- If you configure call preemption using the global parameter and a new Tel Profile is subsequently added, the `TelProfile_CallPriorityMode` parameter automatically acquires the same setting as well.
- This feature is applicable to FXO, CAS, and ISDN interfaces.
- For FXO interfaces, the preemption is done only on existing IP-to-Tel calls. In other words, if all the current FXO channels are busy with calls that were answered by the FXO device (i.e., Tel-to-IP calls), new incoming emergency IP-to-Tel calls are rejected.

### 30.11.4 Enhanced 9-1-1 Support for Lync Server 2010

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.

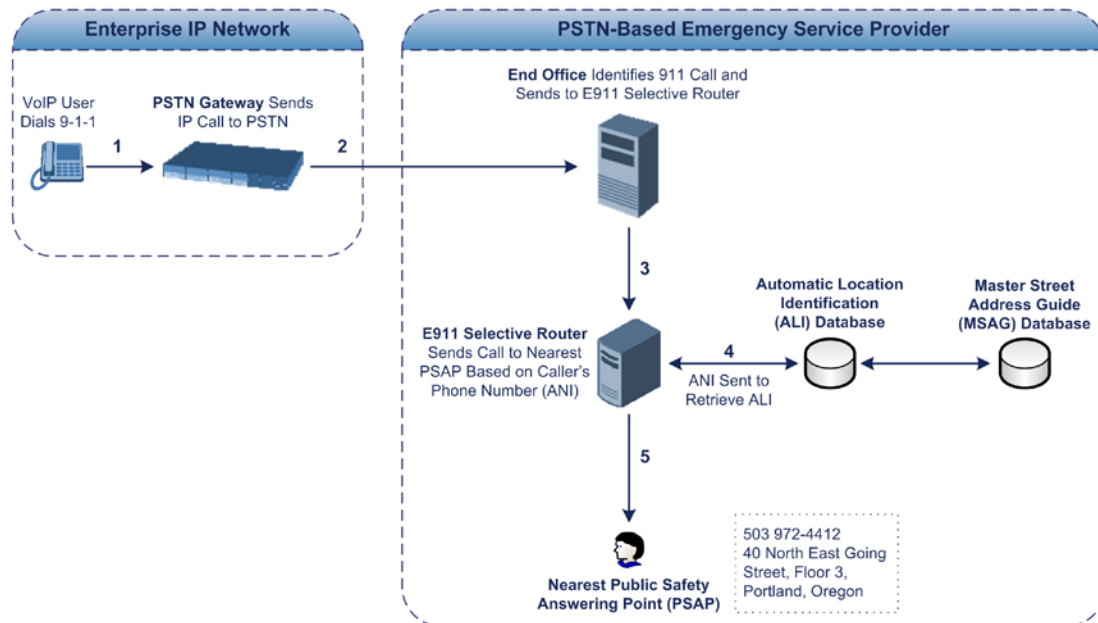
Today, most enterprises implement an IP-based infrastructure providing a VoIP network with fixed and nomadic users, allowing connectivity anywhere with any device. This, together with an often deployed multi-line telephone system (MLTS) poses a challenge for E9-1-1 due to the difficulty in accurately locating the E9-1-1 caller.

This section describes the E9-1-1 solution provided by Microsoft Lync Server 2010 (hereafter referred to as *Lync Server 2010*), and the deployed AudioCodes ELIN Gateway which provides the ISDN (or CAMA) connectivity to the PSTN-based E9-1-1 emergency providers. This section also describes the configuration of AudioCodes ELIN Gateway for interoperating between the Lync Server 2010 environment and the E9-1-1 emergency provider.

#### 30.11.4.1 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:

**Figure 30-6: Call Flow of E9-1-1 to PSTN-Based Emergency Services Provider**

1. The VoIP user dials 9-1-1.
2. The call is eventually sent to the PSTN through a PSTN Gateway.
3. The PSTN 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.

#### 30.11.4.2 Microsoft Lync Server 2010 and E9-1-1

Microsoft Lync Server 2010 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, Lync Server 2010 offers an innovative solution to solving Enterprises E9-1-1 location problems.

##### 30.11.4.2.1 Gathering Location Information of Lync 2010 Clients for 911 Calls

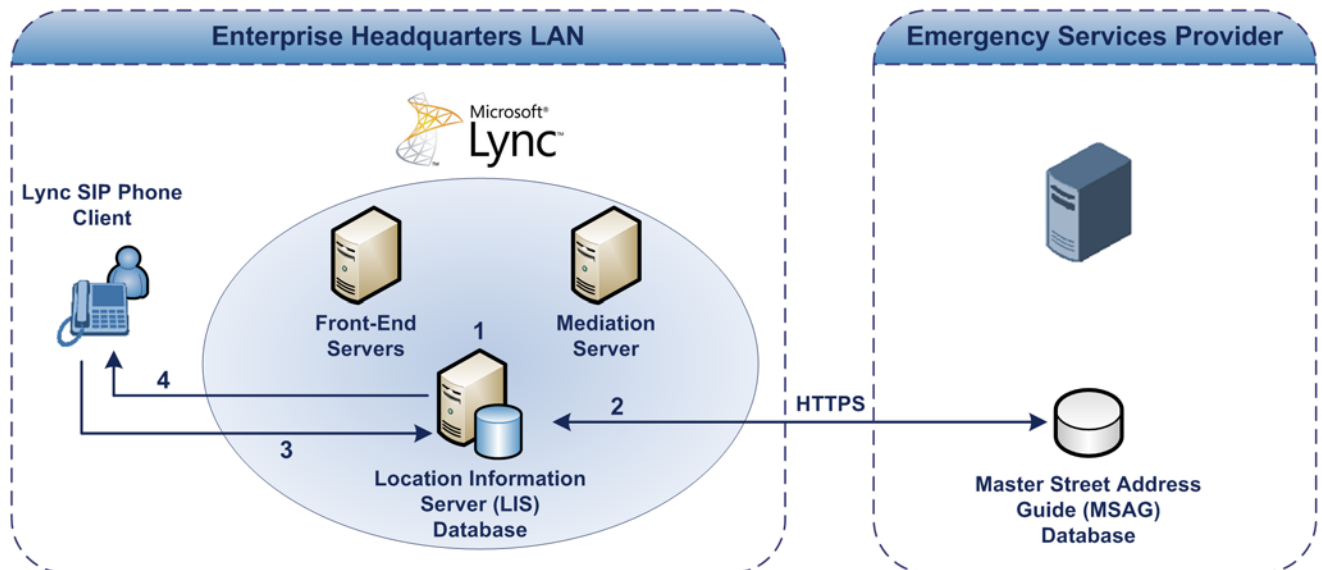
When a Microsoft® Lync™ 2010 client (hereafter referred to as *Lync 2010 client*) is enabled for E9-1-1, the location data that is stored on the client is sent during an emergency call. This stored location information is acquired automatically from the Microsoft Location Information Server (LIS). The LIS stores the location of each network element in the enterprise. Immediately after the Lync 2010 client registration process or



when the operating system detects a network connection change, each Lync 2010 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 Lync 2010 client dials 9-1-1, this location information is then included as part of the emergency call and used by the Emergency Services provider to route the call to the correct PSAP.

The gathering of location information in the Lync Server 2010 network is illustrated in the figure below:

**Figure 30-7: Microsoft Lync Server 2010 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 373.
2. The Administrator validates addresses with the Emergency Services 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 Lync 2010 client initiates a location request to the LIS under the following circumstances:
  - Immediately after startup and registering the user with Lync Server 2010
  - Approximately every four hours after initial registration
  - Whenever a network connection change is detected (such as roaming to a new WAP)

The Lync 2010 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 Lync 2010 client that moves inside the corporate network such as a soft phone on a laptop that connects wirelessly to the corporate network, Lync Server 2010 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 Lync Server 2010 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.

#### 30.11.4.2.2 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.

**Columns in the LIS Database**

Network Element	Columns
<b>Wireless access point</b>	<BSSID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,<PreDirectional>,...<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>
<b>Subnet</b>	<Subnet>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,<PreDirectional>,...<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>
<b>Port</b>	<ChassisID>,<PortIDSubType>,<PortID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,...<PreDirectional>,<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>
<b>Switch</b>	<ChassisID>,<Description>,<Location>,<CompanyName>,<HouseNumber>

Network Element	Columns
	er>,<HouseNumberSuffix>,<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 Gateway, the Administrator must add the ELIN number to the <CompanyName> column (shown in the table above in **bold** typeface). As the ELIN Gateway 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 (xxxxxxxxx).

When the ELIN Gateway 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 Lync Server 2010 location policy, Location Required is set to **Yes** or **Disclaimer**, the user will be prompted to enter a location manually.

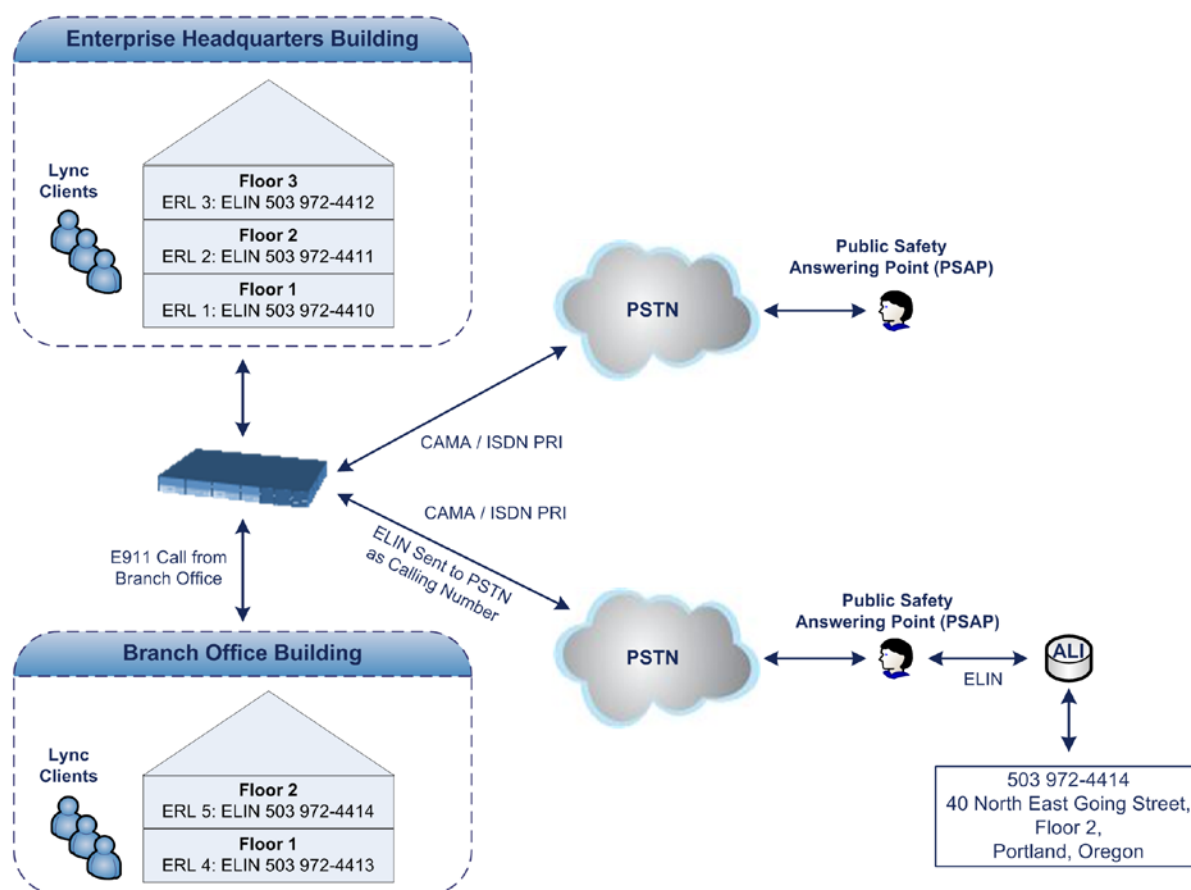
### 30.11.4.2.3 Passing Location Information to the PSTN Emergency Provider

When a Lync 2010 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 PSTN-based Emergency Services provider. The Emergency Services provider then routes the call to the nearest and most appropriate PSAP based on the location information contained within the call.

Lync Server 2010 passes the location information of the Lync 2010 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 PSTN network using ISDN PRI due to protocol limitations. To overcome this, Enterprises using PSTN Gateways 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 Lync Server 2010 sends a SIP INVITE message with the PIDF-LO to the PSTN Gateway, it can parse the content and translate the calling number to an appropriate ELIN. The PSTN Gateway then sends the call to the PSTN with the ELIN number as the calling number. This ELIN number is sent to the Emergency Services 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 30-8: Implementing ERLs and ELINs for E9-1-1 in Lync Server 2010**

The table below shows an example of designating ERLs to physical areas (floors) in a building and associating each ERL with a unique ELIN.

#### 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.

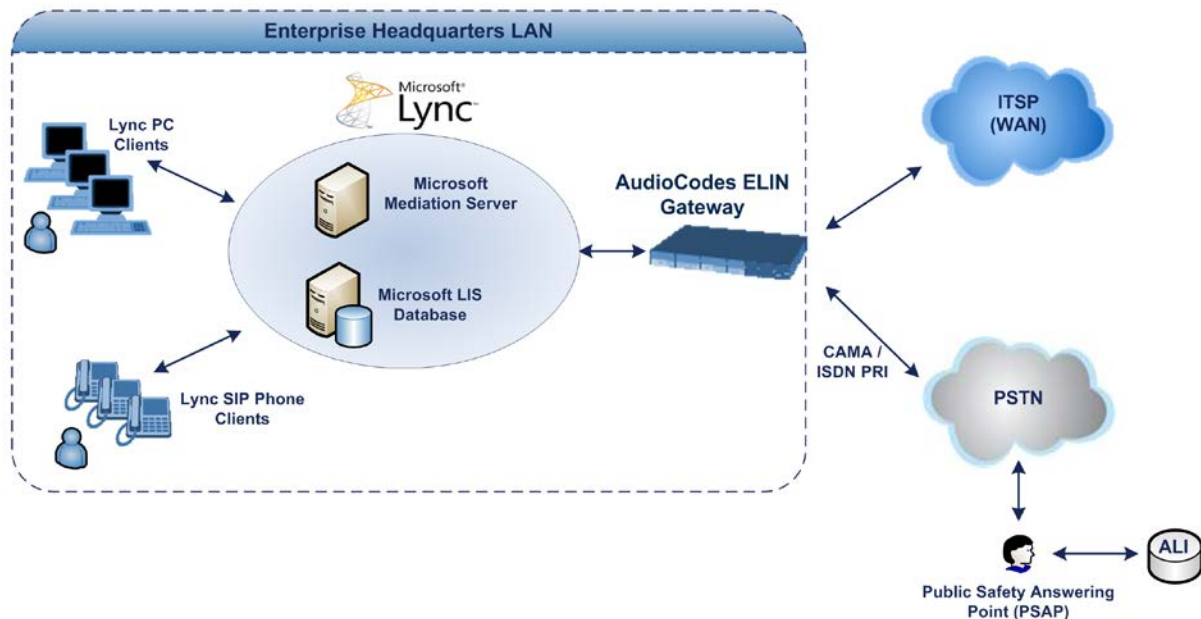
#### 30.11.4.3 AudioCodes ELIN Gateway for Lync Server 2010 E9-1-1 Calls to PSTN

The 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 PSTN network using ISDN PRI due to protocol limitations. To solve this issue, Lync Server 2010 requires a PSTN Gateway (*ELIN Gateway*) to send the E9-1-1 call to the PSTN. When Lync Server 2010 sends the PIDF-LO to the PSTN Gateway, 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 Services provider's ALI database.

The figure below illustrates an AudioCodes ELIN Gateway deployed in the Lync Server 2010 environment for handling E9-1-1 calls between the Enterprise and the PSTN.

**Figure 30-9: AudioCodes ELIN Gateway for E9-1-1 in Lync Server 2010 Environment**



#### 30.11.4.3.1 Detecting and Handling E9-1-1 Calls

The ELIN Gateway identifies E9-1-1 calls and translates their incoming E9-1-1 calling numbers into ELIN numbers, sent toward the PSAP. The ELIN Gateway handles the received E9-1-1 calls as follows:

1. The ELIN Gateway 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/pidf+xml
```

2. The ELIN Gateway 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 ELIN Gateway 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 ELIN Gateway 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 Lync 2010 Clients for Dropped E9-1-1 Calls' on page 378. 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 this 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
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 380), 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 depend on the AudioCodes ELIN Gateway deployed in the Lync Server 2010 environment:

- **Mediant 1000 Series and Mediant 2000:** 100 entries
- **Mediant 3000:** 300 entries

4. The ELIN Gateway uses the ELIN number as the E9-1-1 calling number and sends it in the ISDN Setup message (as an ANI / Calling Party Number) to the PSTN.

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--

```

### 30.11.4.3.2 Pre-empting Existing Calls for E9-1-1 Calls

If the ELIN Gateway receives an E9-1-1 call from the IP network and there are unavailable channels (for example, all busy), the ELIN Gateway 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 channel pertaining to the same Trunk Group for which the E9-1-1 call was initially destined. For example, if an E9-1-1 call is destined for Trunk Group #2 and all the channels belonging to this group are busy, the ELIN Gateway terminates one of the calls in this group to free a channel for accepting the E9-1-1 call.

This feature is initiated only if the received SIP INVITE message contains a *Priority* header set to "emergency", as shown below:

```
PRIORITY: emergency
```

### 30.11.4.3.3 PSAP Callback to Lync 2010 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



ELIN Gateway to translate the ELIN number back into the E9-1-1 caller's extension number.

In the ELIN table of the ELIN Gateway, 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 ELIN Gateway 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 ELIN Gateway is as follows:

1. When the ELIN Gateway receives any call from the PSTN, it searches the ELIN table for an ELIN that corresponds to the received Called Party Number in the incoming PSTN call.
2. If a match is found in the ELIN table, it routes the call to the Mediation Server 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 ELIN Gateway updates the Time in the ELIN table. (The Count is not affected).

The PSAP callback can be done only within a user-defined timeout (see 'Configuring the E9-1-1 Callback Timeout' on page 380) 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 ELIN Gateway 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, then the PSAP callback is routed to this new E9-1-1 caller.

In scenarios where the same ELIN number is being used by multiple E9-1-1 callers, upon receipt of a PSAP callback, the ELIN Gateway 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 ELIN Gateway sends it to the E9-1-1 caller with phone number "4258359555".

**Choosing Caller of ELIN**

ELIN	Time	Call From
4257275678	11:00	4258359333
4257275678	11:01	4258359444
4257275678	11:03	<b>4258359555</b>

#### 30.11.4.3.4 Selecting ELIN for Multiple Calls within Same ERL

The ELIN Gateway 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 ELIN Gateway sends the ELIN number as the E9-1-1 calling number to the PSTN-based emergency provider. If the XML message contains more than one ELIN number, the ELIN Gateway 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 ELIN Gateway 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 ELIN Gateway 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 ELIN Gateway 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 ELIN Gateway selects ELIN 4257275678.

In this scenario, multiple E9-1-1 calls will be sent with the same ELIN.

#### 30.11.4.3.5 Location Based Emergency Routing

The device supports location-based emergency routing (E-911) in Lync Server 2010. This ensures that E-911 calls from remote branches are routed to emergency providers that are relevant to the geographical area in which the remote branch callers are physically located. To support this, the device enables routing and SIP header / number manipulation of such emergency calls based on the geographical location of the caller. The device manipulates the received destination number (i.e., 911) from the remote branch callers, into a destination number of an emergency provider that is relevant to the geographical area in which the remote branch office is located.

### 30.11.4.4 Configuring AudioCodes ELIN Gateway

This section describes E9-1-1 configuration of the AudioCodes ELIN Gateway deployed in the Lync Server 2010 environment.

#### 30.11.4.4.1 Enabling the E9-1-1 Feature

By default, the E9-1-1 feature in the ELIN Gateway for Lync Server 2010 is disabled. To enable it, the following *ini* file parameter setting must be done:

```
E911Gateway = 1
```

#### 30.11.4.4.2 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 interval, by using the following *ini* file parameter:

```
E911CallbackTimeout = <time value> ; where <time value> can be any value from 0 through 60
```

#### 30.11.4.4.3 Configuring the SIP Release Cause Code for Failed E9-1-1 Calls

When a Lync 2010 client makes an emergency call, the call is routed through the Microsoft Mediation Server to the ELIN Gateway, which sends it on to the PSTN. In some scenarios, the call may not be established due to either the PSTN (for example, the destination is busy or not found) or ELIN Gateway (for example, lack of resources or an internal error). In such a scenario, the Mediation Server requires that the ELIN Gateway "reject" the call with the SIP release cause code 503 "Service Unavailable" instead of the designated release call. Such a release cause code enables the Mediation Server to issue a failover to another entity (for example, another ELIN Gateway), instead of retrying the call or returning the release call to the user.



To support this requirement, the ELIN Gateway can be configured to send the 503 "Service Unavailable" release cause code instead of SIP 4xx if an emergency call cannot be established. To enable this support, the following *ini* file parameter setting must be done:



**Note:** This can also be configured using the *ini* file parameter, EmergencySpecialReleaseCause.

➤ **To enable SIP response 503 upon failed E911:**

1. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).
2. From the 'Emergency Special Release Cause' drop-down list, select **Enable**.

#### 30.11.4.4.4 Configuring Location-Based Emergency Routing

The device identifies callers by their ELIN numbers contained in the PIDF-LO XML body of the received SIP INVITE message. To configure the manipulation rule for location-based emergency routing, the ELIN number is used as the source prefix in the Destination Phone Number Manipulation Table for Tel -> IP Calls table. To identify this source prefix as an E-911 ELIN number, the "ELIN" string is added in front of the source prefix number, for example, "ELIN1234567890". For example, assume an E-9-1-1 call is received for destination 911@company.com and the ELIN number is 1234567890; to create the new destination as 15509115000@company.com, the destination number is manipulated using the manipulation table by adding prefix 1550 and suffix 5000.

➤ **To configure location-based emergency routing:**

1. Enable location-based emergency routing, by loading an ini file to the device with the following parameter setting:

```
E911Gateway = 2
```

2. In the Destination Phone Number Manipulation Table for Tel -> IP Calls table (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** > **Dest Number Tel->IP**), configure the following fields:
  - Under the **Rule** tab:
    - ◆ 'Source Prefix': ELIN<ELIN source number>
  - Under the **Action** tab:
    - ◆ Configure the manipulation action as required

#### 30.11.4.4.5 Viewing the ELIN Table

You can view the ELIN table of the ELIN Gateway. The method depends on the type of device:

- Using the following CLI command:

```
# show voip gw 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
```

## 30.12 Multilevel Precedence and Preemption

The device supports Multilevel Precedence and Preemption (MLPP) service. MLPP is a call priority scheme, which does the following:

- Assigns a precedence level (priority level) to specific phone calls or messages.
- Allows higher priority calls (*precedence call*) and messages to preempt lower priority calls and messages (i.e., terminates existing lower priority calls) that are recognized within a user-defined domain (*MLPP domain ID*). The domain specifies the collection of devices and resources that are associated with an MLPP subscriber. When an MLPP subscriber that belongs to a particular domain places a precedence call to another MLPP subscriber that belongs to the same domain, MLPP service can preempt the existing call that the called MLPP subscriber is on for a higher-precedence call. MLPP service availability does not apply across different domains.

MLPP is typically used in the military where, for example, high-ranking personnel can preempt active calls during network stress scenarios such as a national emergency or degraded network situations.

MLPP can be enabled for all calls, using the global parameter, `CallPriorityMode`, or for specific calls using the Tel Profile parameter, `CallPriorityMode`.



### Notes:

- For Trunk Groups configured with call preemption, all must be configured to MLPP [1] or all configured to Emergency [2]. In other words, you cannot set some trunks to [1] and some to [2].
- The global parameter must be set to the same value as that of the Tel Profile parameter; otherwise, the Tel Profile parameter is not applied.
- If you configure call preemption using the global parameter and a new Tel Profile is subsequently added, the `TelProfile_CallPriorityMode` parameter automatically acquires the same setting as well.

The Resource Priority value in the Resource-Priority SIP header can be any one of those listed in the table below. A default MLPP call Precedence Level (configured by the `SIPDefaultCallPriority` parameter) is used if the incoming SIP INVITE or PRI Setup message contains an invalid priority or Precedence Level value respectively. For each MLPP call priority level, the Multiple Differentiated Services Code Points (DSCP) can be set to a value from 0 to 63.

**MLPP Call Priority Levels (Precedence) and DSCP Configuration Parameters**

MLPP Precedence Level	Precedence Level in Resource-Priority SIP Header	DSCP Configuration Parameter
0 (lowest)	routine	MLPPRoutineRTPDSCP
2	priority	MLPPPriorityRTPDSCP
4	immediate	MLPPImmediateRTPDSCP
6	flash	MLPPFlashRTPDSCP
8	flash-override	MLPPFlashOverRTPDSCP
9 (highest)	flash-override-override	MLPPFlashOverOverRTPDSCP

The device automatically interworks the network identity digits (NI) in the ISDN Q.931 Precedence Information Element (IE) to the network domain subfield of the INVITE's Resource-Priority header, and vice versa. The SIP Resource-Priority header contains two fields, namespace and priority. The namespace is subdivided into two subfields, network-domain and precedence-domain. Below is an example of a Resource-Priority header whose network-domain subfield is "uc", r-priority field is "priority" (2), and precedence-domain subfield is "000000":

Resource-Priority: uc-000000.2

The MLPP Q.931 Setup message contains the Precedence IE. The NI digits are presented by four nibbles found in octets 5 and 6. The device checks the NI digits according to the translation table of the Department of Defense (DoD) Unified Capabilities (UC) Requirements (UCR 2008, Changes 3) document, as shown below:

**NI Digits in ISDN Precedence**

Level IE	Network Domain in SIP Resource-Priority Header
0000	uc
0001	cuc
0002	dod
0003	nato

**Notes:**

- If the received ISDN message contains NI digits that are not listed in the translation table, the device sets the network-domain to "uc" in the outgoing SIP message.
- If the received SIP message contains a network-domain value that is not listed in the translation table, the device sets the NI digits to "0000" in the outgoing ISDN message.
- If the received ISDN message does not contain a Precedence IE, you can configure the namespace value - dsn (default), dod, drsn, uc, or cuc - in the SIP Resource-Priority header of the outgoing INVITE message. This is done using the MLPPDefaultNamespace parameter. You can also configure up to 32 user-defined namespaces, using the table ini file parameter, ResourcePriorityNetworkDomains. Once defined, you need to set the MLPPDefaultNamespace parameter value to the desired table row index.



By default, the device maps the received Resource-Priority field of the SIP Resource-Priority header to the outgoing ISDN PRI Precedence Level (priority level) field as follows:

- If the network-domain field in the Resource-Priority header is "uc", then the device sets the Precedence Level field in the ISDN PRI Precedence Level IE according to Table 5.3.2.12-4 (Mapping of RPH r-priority Field to PRI Precedence Level Value):

**Mapping of SIP Resource-Priority Header to PRI Precedence Level for MLPP**

MLPP Precedence Level	PRI Precedence Level	SIP Resource-Priority Header Field
Routine	4	0
Priority	3	2
Immediate	2	4

MLPP Precedence Level	PRI Precedence Level	SIP Resource-Priority Header Field
Flash	1	6
Flash Override	0	8

- If the network-domain field in the Resource-Priority header is any value other than "uc", then the device sets the Precedence Level field to "0 1 0 0" (i.e., "routine").

This can be modified using the EnableIp2TelInterworkingtable field of the ini file parameter, ResourcePriorityNetworkDomains.



#### Notes:

- If required, you can exclude the "resource-priority" tag from the SIP Require header in INVITE messages for Tel-to-IP calls when MLPP priority call handling is used. This is configured using the RPRequired parameter.
- For a complete list of the MLPP parameters, see 'MLPP and Emergency Call Parameters' on page 788.

## 30.12.1 MLPP Preemption Events in SIP Reason Header

The device sends the SIP Reason header (as defined in RFC 4411) to indicate the reason and type of a preemption event. The device sends a SIP BYE or CANCEL request, or SIP 480, 486, 488 response (as appropriate) with a Reason header whose Reason-params can include one of the following preemption cause classes:

- Reason: preemption ;cause=1 ;text="UA Preemption"
- Reason: preemption ;cause=2 ;text="Reserved Resources Preempted"
- Reason: preemption ;cause=3 ;text="Generic Preemption"
- Reason: preemption ;cause=4 ;text="Non-IP Preemption"

This Reason cause code indicates that the session preemption has occurred in a non-IP portion of the infrastructure. The device sends this code in the following scenarios:

- The device performs a network preemption of a busy call (when a high priority call is received), the device sends a SIP BYE or CANCEL request with this Reason cause code.
- The device performs a preemption of a B-channel for a Tel-to-IP outbound call request from the softswitch for which it has not received an answer response (e.g., Connect), and the following sequence of events occurs:
  - a. The device sends a Q.931 DISCONNECT over the ISDN MLPP PRI to the partner switch to preempt the remote end instrument.
  - b. The device sends a 488 (Not Acceptable Here) response with this Reason cause code.
- Reason: preemption; cause=5; text="Network Preemption"

This Reason cause code indicates preempted events in the network. Within the Defense Switched Network (DSN) network, the following SIP request messages and response codes for specific call scenarios have been identified for signaling this preemption cause:

- SIP:BYE - If an active call is being preempted by another call
- CANCEL - If an outgoing call is being preempted by another call

- 480 (Temporarily Unavailable), 486 (User Busy), 488 (Not Acceptable Here) - Due to incoming calls being preempted by another call.

The device receives SIP requests with preemption reason cause=5 in the following cases:

- The softswitch performs a network preemption of an active call - the following sequence of events occurs:
  - a. The softswitch sends the device a SIP BYE request with this Reason cause code.
  - b. The device initiates the release procedures for the B-channel associated with the call request and maps the preemption cause to PRI Cause = #8 'Preemption'. This value indicates that the call is being preempted. For PRI, it also indicates that the B-channel is not reserved for reuse.
  - c. The device sends a SIP 200 OK in response to the received BYE, before the SIP end instrument can proceed with the higher precedence call.
- The softswitch performs a network preemption of an outbound call request for the device that has not received a SIP 2xx response - the following sequence of events occur:
  - a. The softswitch sends the device a SIP 488 (Not Acceptable Here) response code with this Reason cause code. The device initiates the release procedures for the B-channel associated with the call request and maps the preemption cause to PRI Cause = #8 'Preemption'.
  - b. The device deactivates any user signaling (e.g., ringback tone) and when the call is terminated, it sends a SIP ACK message to the softswitch.

### 30.12.2 Precedence Ring Tone

You can assign a ring tone that is defined in the CPT file to be played when a precedence call is received from the IP side. This is configured by the PrecedenceRingingType parameter. You can configure the duration for which the device plays a preemption tone to the Tel and IP sides if a call is preempted, using the PreemptionToneDuration parameter.

Emergency Telecommunications Services (ETS) calls (e.g., E911) can be configured with a higher priority than any MLPP call (default), using the E911MLPPBehavior parameter.

## 30.13 Denial of Collect Calls

You can configure the device to reject (disconnect) incoming Tel-to-IP collect calls and to signal this denial to the PSTN. This capability is required, for example, in the Brazilian telecommunication system to deny collect calls. When this feature is enabled upon rejecting the incoming call, the device sends a sequence of signals to the PSTN. This consists of an off-hook, an on-hook after one second, and then an off-hook after two seconds. In other words, this is in effect, a double-answer sequence.

This feature can be enabled for all calls, using the EnableFXODoubleAnswer "global" parameter, or it can be enabled for specific calls, by enabling this feature in a Tel Profile.



#### Notes:

- This feature is applicable only to FXO interfaces.
- If automatic dialing is also configured for an FXO port enabled with Denial of Collect Calls, the FXO line does not answer the incoming call (ringing) until a SIP 200 OK is received from the remote destination. When a 200 OK is received, a double answer is sent from the FXO line.
- Ensure that the PSTN side is configured to identify this double-answer signal.

## 30.14 Configuring ISDN Supplementary Services

The ISDN Supp Services Table page allows you to configure supplementary services for Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) phones connected to the device. This feature enables the device to route IP-to-Tel calls (including voice and fax) to specific BRI ports (channels).

This table allows you to define BRI phone extension numbers per BRI port pertaining to a specific BRI module. Therefore, this offers support for point-to-multipoint configuration of several phone numbers per BRI channel. Up to eight phone numbers can be defined per BRI trunk. For each BRI endpoint, the following optional configurations can also be defined:

- User ID and password - for registering the BRI endpoint to a third-party softswitch for authentication and/or billing. For viewing BRI registration status, see 'Viewing Endpoint Registration Status' on page 595.
- Caller ID name - for displaying the BRI endpoint's caller ID to a dialed destination, if enabled (i.e., "Presentation" is not restricted)
- Caller ID presentation or restriction
- Enable/disable sending caller ID to BRI endpoints

### Notes:

- To use this table for routing of IP-to-Tel calls to specific BRI channels, the Channel Select Mode in the Hunt Group Settings must be set to 'Select Trunk by ISDN Supplementary Services Table' (see 'Configuring Hunt Group Settings' on page 291).
- The ISDN Supp Services table can also be configured using the table ini file parameter, ISDNSuppServ or CLI command, configure voip > gw digitalgw isdn-supp-serv.
- To allow the end-user to hear a dial tone when picking up the BRI phone, it is recommended to set the Progress Indicator in the Setup Ack bit (0x10000=65536). Therefore, the recommended value is 0x10000 + 0 x1000 = 65536 + 4096 = 69632 (i.e., set the ISDNInCallsBehavior parameter to 69632).



### ➤ To configure BRI supplementary services:

1. Open the ISDN Supp Services Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Digital Gateway** > **ISDN Supp Services**).

Figure 30-10: ISDN Supp Services Table Page

Index	Phone Number	Module	Port	User ID
1 <input type="radio"/>	4112	1	3	mike
2 <input type="radio"/>		0	0	

↓

User Password	Caller ID	Presentation Restricted	Caller ID Enabled
*	mike	Allowed	Enabled
*		Not Configured	Not Configured

2. Configure the parameters as described in the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.
5. To register the BRI endpoints, click the **Register** button. To unregister the BRI endpoints, click **Unregister**. The registration method for each BRI endpoint is according to the setting of the 'Registration Mode' parameter in the Trunk Group Settings page.

ISDN Supp Services Table Parameters

Parameter	Description
Phone Number CLI: phone-number <b>[ISDNSuppServ_PhoneNumber]</b>	Defines the telephone extension number for the BRI endpoint.
Module CLI: module <b>[ISDNSuppServ_Module]</b>	Defines the BRI module number to which the BRI extension pertains.
Port CLI: port <b>[ISDNSuppServ_Port]</b>	Defines the port number on the BRI module to which the BRI extension is connected.
User ID CLI: user-id <b>[ISDNSuppServ_UserId]</b>	Defines the User ID for registering the BRI endpoint to a third-party softswitch for authentication and/or billing.
User Password CLI: user-password <b>[ISDNSuppServ_UserPassword]</b>	Defines the user password for registering the BRI endpoint to a third-party softswitch for authentication and/or billing. <b>Note:</b> For security, the password is displayed as an asterisk (*).
Caller ID Number CLI: caller-id-number <b>[ISDNSuppServ_CallerID]</b>	Defines the caller ID name of the BRI extension (sent to the IP side). The valid value is a string of up to 18 characters.
Presentation Restricted CLI: presentation-restricted <b>[ISDNSuppServ_IsPresentationRestricted]</b>	Determines whether the BRI extension sends its Caller ID information to the IP when a call is made. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Allowed = The device sends the string defined in the 'Caller ID' field when this BRI extension makes a Tel-to-IP call.</li> <li>▪ <b>[1]</b> Restricted = The string defined in the 'Caller ID' field is not sent.</li> </ul>
Caller ID Enabled CLI: caller-id-enable <b>[ISDNSuppServ_IsCallerIDEnabled]</b>	Enables the receipt of Caller ID. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disabled = The device does not send Caller ID information to the BRI extension.</li> <li>▪ <b>[1]</b> Enabled = The device sends Caller ID information to the BRI extension</li> </ul>



## 30.15 Advice of Charge Services for Euro ISDN

Advice of charge (AOC) is a pre-billing function that tasks the rating engine with calculating the cost of using a service and relaying that information back to the customer thus, allowing users to obtain charging information for all calls during the call (AOC-D) or at the end of the call (AOC-E), or both.

The AOC-D and AOC-E messages are part of the Facility Information Element (IE) message:

- AOC-D message—ISDN Advice of Charge information sent during a call. The message is sent periodically to subscribers of AOC during-call services.
- AOC-E message—ISDN Advice of Charge information sent at the end of a call.

The device supports the sending of AoC messages for Tel-to-IP calls, providing billing applications with the number of charged units. This feature can typically be implemented in the hotel industry, where external calls made by guests can be billed accurately. In such a setup, the device is connected on one side to a PBX through an E1 line (Euro ISDN), and on the other side to a SIP trunk provided by an ITSP. When a call is made by a guest, the device first sends an AOC-D Facility message to the PBX indicating the connection charge unit, and then sends subsequent AOC-D messages every user-defined interval to indicate the charge unit during the call. When the call ends, the device sends an AoC-E Facility message to the PBX indicating the total number of charged units.

To configure AoC:

1. Ensure that the PSTN protocol for the E1 trunk line is Euro ISDN and set to network side.
2. Ensure that the date and time of the device is correct. For accuracy, it is recommended to use an NTP server to obtain the date and time.
3. Enable the AoC service, using the EnableAOC parameter.
4. Configure charge codes in the Charge Code table (ChargeCode) - see [Configuring Charge Codes](#) on page 393. Note that in the Charge Code table, the table fields are as follows:
  - 'End Time' - time at which this charge code ends
  - 'Pulse Interval' - time between every sent AOC-D Facility message
  - 'Pulses On Answer' - number of charging units in first generated AOC-D Facility message
5. Assign the charge code index to the desired routing rule in the Outbound IP Routing table (see '[Configuring Outbound IP Routing Table](#)' on page 321).



## 30.16 Configuring Voice Mail

The Voice Mail Settings page allows you to configure the voice mail parameters. For a description of these parameters, see 'Configuration Parameters Reference' on page 661.



### Notes:

- The Voice Mail Settings page is available only for FXO and CAS interfaces.
- For more information on configuring voice mail, refer to the *CPE Configuration Guide for Voice Mail User's Manual*.

### ➤ To configure the Voice Mail parameters:

1. Open the Voice Mail Settings page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Advanced Applications** > **Voice Mail Settings**).

Line Transfer Mode	None	▼
Voice Mail Interface	NONE	▼
▼ Digit Patterns		
Forward on Busy Digit Pattern (Internal)	<input type="text"/>	
Forward on No Answer Digit Pattern (Internal)	<input type="text"/>	
Forward on Do Not Disturb Digit Pattern (Internal)	<input type="text"/>	
Forward on No Reason Digit Pattern (Internal)	<input type="text"/>	
Forward on Busy Digit Pattern (External)	<input type="text"/>	
Forward on No Answer Digit Pattern (External)	<input type="text"/>	
Forward on Do Not Disturb Digit Pattern (External)	<input type="text"/>	
Forward on No Reason Digit Pattern (External)	<input type="text"/>	
Internal Call Digit Pattern	<input type="text"/>	
External Call Digit Pattern	<input type="text"/>	
Disconnect Call Digit Pattern	<input type="text"/>	
Digit To Ignore Digit Pattern	<input type="text"/>	
▼ Message Waiting Indication (MWI)		
MWI Off Digit Pattern	<input type="text"/>	
MWI On Digit Pattern	<input type="text"/>	
MWI Suffix Pattern	<input type="text"/>	
MWI Source Number	<input type="text"/>	
▼ SMDI		
⚡ Enable SMDI	Disable	▼
SMDI Timeout [msec]	2000	

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## Reader's Notes

## 31 Analog Gateway

This section describes configuration of analog settings.



**Note:** The Analog Gateway submenu appears only if the device is installed with an FXS or FXO module.

### 31.1 Configuring Keypad Features

The Keypad Features page enables you to activate and deactivate the following features directly from the connected telephone's keypad:

- Call Forward
- Caller ID Restriction
- Hotline for automatic dialing
- Call Transfer
- Call Waiting
- Rejection of Anonymous Calls



**Notes:**

- The Keypad Features page is available only for FXS interfaces.
- The method used by the device to collect dialed numbers is identical to the method used during a regular call (i.e., max digits, interdigit timeout, digit map, etc.).
- The activation of each feature remains in effect until it is deactivated (i.e., not deactivated after a call).
- For a description of the keypad parameters, see 'Telephone Keypad Sequence Parameters' on page [844](#).

➤ **To configure the keypad features**

1. Open the Keypad Features page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Analog Gateway** > **Keypad Features**).

**Figure 31-1: Keypad Features Page**

▼ Forward	
Unconditional	<input type="text"/>
No Answer	<input type="text"/>
On Busy	<input type="text"/>
On Busy or No Answer	<input type="text"/>
Do Not Disturb	<input type="text"/>
Deactivate	<input type="text"/>
▼ Caller ID Restriction	
Activate	<input type="text"/>
Deactivate	<input type="text"/>
▼ Hotline	
Activate	<input type="text"/>
Deactivate	<input type="text"/>
▼ Transfer	
Blind	<input type="text"/>
▼ Call Waiting	
Activate	<input type="text"/>
Deactivate	<input type="text"/>
▼ Reject Anonymous Call	
Activate	<input type="text"/>
Deactivate	<input type="text"/>

2. Configure the keypad features as required.
3. Click **Submit** to apply your changes.

## 31.2 Configuring Metering Tones

The FXS interfaces can generate 12/16 KHz metering pulses toward the Tel side (e.g., for connection to a pay phone or private meter). Tariff pulse rate is determined according to the device's Charge Codes table. This capability enables users to define different tariffs according to the source/destination numbers and the time-of-day. The tariff rate includes the time interval between the generated pulses and the number of pulses generated on answer.



**Notes:**

- The Metering Tones page is available only for FXS interfaces.
- Charge Code rules can be assigned to routing rules in the Outbound IP Routing Table (see 'Configuring Outbound IP Routing Table' on page 321). When a new call is established, the Outbound IP Routing Table is searched for the destination IP address. Once a route is located, the Charge Code (configured for that route) is used to associate the route with an entry in the Charge Codes table.

➤ **To configure Metering tones:**

1. Open the Metering Tones page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Analog Gateway** > **Metering Tones**).

**Figure 31-2: Metering Tones Page**

Generate Metering Tones	Disable
Metering Tone Type	16 KHz
Charge Codes Table	

2. Configure the Metering tones parameters as required. For a description of the parameters appearing on this page, see 'Configuration Parameters Reference' on page 661.
3. Click **Submit** to apply your changes.
4. To save the changes to the flash memory, see 'Saving Configuration' on page 532.

If you set the 'Generate Metering Tones' parameter to **Internal Table**, access the Charge Codes Table page by clicking the **Charge Codes Table** button. For more information on configuring the Charge Codes table, see 'Configuring Charge Codes' on page 393.

## 31.3 Configuring Charge Codes

The Charge Codes table is used to configure the metering tones (and their time interval) that the FXS interfaces generate to the Tel side. To associate a charge code to an outgoing Tel-to-IP call, use the Outbound IP Routing Table.

You can configure up to 25 different charge codes, where each table row represents a charge code. Each charge code can include up to four different time periods in a day (24 hours). The device selects the time period by comparing the device's current time to the end time of each time period of the selected Charge Code. The device generates the Number of Pulses on Answer once the call is connected and from that point on, it generates a pulse each Pulse Interval. If a call starts at a certain time period and crosses to the next, the information of the next time period is used.



**Notes:**

- The Charge Codes Table page is available only for FXS interfaces.
- The Charge Codes table can also be used to configure Advice of Charge (AoC) services for Euro ISDN trunks (see Advice of Charge Services for Euro ISDN on page 388).
- The Charge Codes table can also be configured using the table ini file parameter, ChargeCode or CLI command, configure voip > gw analoggw charge-code.

➤ **To configure the Charge Codes:**

1. Open the Charge Codes Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Charge Codes**). Alternatively, you can access this page from the Metering Tones page (see 'Configuring Metering Tones' on page 392).

**Figure 31-3: Charge Codes Table Page**

Table Index													0-4
Index	Time Period 1			Time Period 2			Time Period 3			Time Period 4			
	End Time	Pulse Interval	Pulses On Answer	End Time	Pulse Interval	Pulses On Answer	End Time	Pulse Interval	Pulses On Answer	End Time	Pulse Interval	Pulses On Answer	
0	07	30	1	14	20	2	20	15	1	00	60	1	
1	05	60	1	14	20	1	00	60	1				
2	00	60	1										
3													
4													

2. Configured the charge codes, as required. For a description of the parameters, see the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to the flash memory, see 'Saving Configuration' on page 532.

**Charge Codes Table Parameter Description**

Parameter	Description
End Time CLI: end-time-<1-4> [ChargeCode_EndTime<1-4>]	Defines the end of the time period in a 24 hour format, <i>hh</i> . For example, "04" denotes 4 A.M. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ The first time period always starts at midnight (00).</li> <li>▪ It is mandatory that the last time period of each rule end at midnight (00). This prevents undefined time frames in a day.</li> </ul>
Pulse Interval CLI: pulse-interval-<1-4> [ChargeCode_PulseInterval<1-4>]	Defines the time interval between pulses (in tenths of a second).
Pulses On Answer CLI: pulses-on-answer-<1-4> [ChargeCode_PulsesOnAnswer<1-4>]	Defines the number of pulses sent on answer.

## 31.4 Configuring FXO Settings

The FXO Settings page allows you to configure the device's specific FXO parameters. For a description of these parameters, see 'Configuration Parameters Reference' on page 661.



**Note:** The FXO Settings page is available only for FXO interfaces.

➤ **To configure the FXO parameters:**

1. Open the FXO Settings page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Analog Gateway** > **FXO Settings**).

**Figure 31-4: FXO Settings Page**

Dialing Mode	Two Stages	▼
Waiting for Dial Tone	No	▼
Time to Wait before Dialing [msec]	1000	
Ring Detection Timeout [sec]	8	
Reorder Tone Duration [sec]	255	
Answer Supervision	No	▼
Rings before Detecting Caller ID	1	▼
Send Metering Message to IP	No	▼
Disconnect Call on Busy Tone Detection (CAS)	Enable	▼
Disconnect On Dial Tone	Disable	▼
Guard Time Between Calls	1	
FXO Double Answer	Disable	▼
FXO AutoDial Play BusyTone	Disable	▼

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 31.5 Configuring Authentication

The Authentication page [defines](#) a user name and password for authenticating each device port. Authentication is typically used for FXS interfaces, but can also be used for FXO interfaces.



**Notes:**

- For configuring whether authentication is done per port or for the entire device, use the parameter AuthenticationMode.
- If authentication is configured for the entire device, the configuration in this table is ignored.
- If the user name or password is not configured in this table, the port's phone number (configured in the Trunk Group Table) and global password (configured by the global parameter, Password) are used instead for authentication of the port.
- After you click **Submit**, the password is displayed as an asterisk (\*).
- The Authentication table can also be configured using the table ini file parameter, Authentication (see 'Configuration Parameters Reference' on page 661) or CLI command, configure voip > gw analoggw authentication.

- **To configure authentication credentials per port:**
- Set the parameter 'Registration Mode' (AuthenticationMode) to **Per Endpoint**. This can be configured in any of the following pages:
    - Proxy & Registration page (see 'Configuring Proxy and Registration Parameters' on page 222).
    - Trunk Group Settings page (see 'Configuring Hunt Group Settings' on page 291), where registration method is configured per Trunk Group.
  - Open the Authentication page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Analog Gateway** > **Authentication**).

**Figure 31-5: Authentication Page**

Gateway Port	User Name	Password
Module 1 Port 1 FXS	<input type="text" value="user1"/>	<input type="password" value="skkkskksk"/>
Module 1 Port 2 FXS	<input type="text" value="user2"/>	<input type="password" value="skkkskksk"/>
Module 2 Port 1 FXO	<input type="text"/>	<input type="password"/>
Module 2 Port 2 FXO	<input type="text"/>	<input type="password"/>
Module 2 Port 3 FXO	<input type="text"/>	<input type="password"/>
Module 2 Port 4 FXO	<input type="text"/>	<input type="password"/>

- Configure port authentication credentials as required. For a description of the parameters, see the table below.
- Click **Submit** to apply your changes.

**Authentication Table Parameter Description**

Parameter	Description
CLI: port [Authentication_Port]	Defines the port to authenticate. <b>Note:</b> This parameter is not relevant to the Web interface.
CLI: port-type [Authentication_Module]	Defines the module number on which the port is located. <b>Note:</b> This parameter is not relevant to the Web interface.
User Name CLI: user-name [Authentication_UserId]	Defines the user name used for authenticating the port.
Password CLI: password [Authentication_UserPassword]	Defines the password used for authenticating the port.

## 31.6 Configuring Automatic Dialing

The Automatic Dialing page allows you to define a telephone number that is automatically dialed when an FXS or FXO port goes off-hook. The dialing can be done immediately upon off-hook, or after a user-defined interval after off-hook referred to as *Hotline* dialing.



**Note:** The Automatic Dialing can also be configured using the table ini file parameter, TargetOfChannel or CLI command, configure voip > gw analoggw automatic-dialing.



➤ **To configure automatic dialing per port:**

1. Open the Automatic Dialing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** > **Automatic Dialing**).

**Figure 31-6: Automatic Dialing Page**

Gateway Port				Destination Phone Number	Auto Dial Status	Hotline Dial Tone Duration [sec]
Module	3	Port	1 FXS	911	Hotline ▼	15
Module	3	Port	2 FXS	200	Enable ▼	0
Module	3	Port	3 FXS		Enable ▼	0
Module	3	Port	4 FXS		Enable ▼	0

The first table entry in the figure above enables Hotline automatic dialing for an FXS port, whereby if the port is off-hooked for over 15 seconds, the device automatically dials 911.

2. Configure automatic dialing per port, as required. See the table below for parameter descriptions.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

**Automatic Dialing Table Parameter Description**

Parameter	Description
Gateway Port [TargetOfChannel_Module] CLI: port [TargetOfChannel_Port]	Lists the FXS or FXO port (per module) for which you want to configure automatic dialing.
Destination Phone Number CLI: /dst-number [TargetOfChannel_Destination]	Defines the destination telephone number to automatically dial.
Auto Dial Status CLI: auto-dial-status [TargetOfChannel_Type]	<p>Enables automatic dialing.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Disable</b> = Automatic dialing for the specific port is disabled.</li> <li>▪ <b>[1] Enable</b> = (Default) Automatic dialing is enabled and the phone number configured in the 'Destination Phone Number' field is automatically dialed if the following occurs: <ul style="list-style-type: none"> <li>✓ FXS interfaces: The phone is off-hooked</li> <li>✓ FXO interfaces: A ring signal (from a PBX/PSTN switch) is detected on the FXO line. The device initiates a call to the destination without seizing the FXO line. The line is seized only after the SIP call is answered.</li> </ul> </li> <li>▪ <b>[2] Hotline</b> = Automatic dialing is done after an interval configured by the 'Hotline Dial Tone Duration' parameter: <ul style="list-style-type: none"> <li>✓ FXS interfaces: When the phone is off-hooked and no digit is dialed within a user-defined time, the configured destination number is automatically dialed.</li> <li>✓ FXO interfaces: If a ring signal is detected, the device seizes the FXO line, plays a dial tone, and then waits for DTMF digits. If no digits are detected within a user-defined time, the configured destination number is automatically dialed by sending a SIP INVITE message with this number.</li> </ul> </li> </ul>

Parameter	Description
Hotline Dial Tone Duration CLI: hotline-dia-ltone-duration [TargetOfChannel_HotLineToneDuration]	<p>Defines the duration (in seconds) after which the destination phone number is automatically dialed. This is applicable only if the port has been configured for Hotline (i.e., 'Auto Dial Status' is set to <b>Hotline</b>).</p> <p>The valid value is 0 to 60. The default is 16.</p> <p><b>Note:</b> You can configure this Hotline interval for all ports, using the global parameter, HotLineToneDuration.</p>

## 31.7 Configuring Caller Display Information

The Caller Display Information table allows you to define a caller identification string (Caller ID) for FXS and FXO ports and enable the device to send the Caller ID to the IP when a call is made. The called party can use this information for caller identification.

The device sends the configured caller ID in the outgoing INVITE message's From header. For information on Caller ID restriction according to destination/source prefixes, see 'Configuring Source/Destination Number Manipulation' on page 297.



### Notes:

- If an FXS port receives 'Private' or 'Anonymous' strings in the SIP From header, the calling name or number is not sent to the Caller ID display.
- If Caller ID is detected on an FXO line (EnableCallerID = 1), it is used instead of the Caller ID configured in this table.
- If you set the 'Caller ID/Name' parameter to the strings "Private" or "Anonymous", Caller ID is restricted and the settings of the 'Presentation' parameter is ignored.
- The Caller Display Information table can also be configured using the table ini file parameter, CallerDisplayInfo or CLI command, configure voip > gw analoggw caller-display-info.

### ➤ To configure Caller Display:

1. Open the Caller Display Information page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Analog Gateway** > **Caller Display Information**).

**Figure 31-7: Caller Display Information Page**

Gateway Port	Caller ID/Name	Presentation
Module 1 Port 1 FXS	Private	Restricted ▼
Module 1 Port 2 FXS	Susan C.	Restricted ▼
Module 2 Port 1 FXO	Lee P.	Allowed ▼
Module 2 Port 2 FXO	Ronaldo	Allowed ▼
Module 2 Port 3 FXO		Allowed ▼
Module 2 Port 4 FXO		Allowed ▼

2. Configure the table as required. For a description of the parameters, see the table below.
3. Click **Submit** to apply your changes.

Caller Display Parameter Description

Parameter	Description
Gateway Port CLI: port [CallerDisplayInfo_Port] [CallerDisplayInfo_Module]	Displays the port per module.
Caller ID/Name CLI: display-string [CallerDisplayInfo_DisplayString]	Defines the Caller ID string. The valid value is a string of up to 18 characters.
Presentation CLI: presentation [CallerDisplayInfo_IsCidRestricted]	<p>Enables the sending of the caller ID string.</p> <ul style="list-style-type: none"> <li>[0] Allowed = The caller ID string is sent when a Tel-to-IP call is made.</li> <li>[1] Restricted = The caller ID string is not sent.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is overridden by the 'Presentation' parameter in the Source Number Manipulation table (see 'Configuring Source/Destination Number Manipulation' on page 297).</li> <li>If this parameter is set to <b>Restricted</b>, the Caller ID is sent to the remote side using only the SIP P-Asserted-Identity or P-Preferred-Identity headers (AssertedIdMode).</li> </ul>

## 31.8 Configuring Call Forward

The Call Forwarding table allows you to configure call forwarding per port for IP-to-Tel calls. This redirects the call (using SIP 302 response) initially destined to a specific device Tel port, to a different device port or to an IP destination.



### Notes:

- To enable call forwarding, set the 'Enable Call Forward' parameter to **Enable**. This is done in the Supplementary Services page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **DTMF and Supplementary** > **Supplementary Services**).
- The Call Forward table can also be configured using the table ini file parameter, FwdInfo or CLI command, configure voip > gw analoggw call-forward.

➤ **To configure Call Forward per port:**

1. Open the Call Forward Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Analog Gateway** > **Call Forward**).

**Figure 31-8: Call Forward Table Page**

Gateway Port	Forward Type	Forward to Phone Number	Time for No Reply Forward
Module 1 Port 1 FXS	On busy	201	30
Module 1 Port 2 FXS	Unconditional	202@10.2.1.1	30
Module 2 Port 1 FXO	No Answer	203	30
Module 2 Port 2 FXO	Deactivate		30
Module 2 Port 3 FXO	Deactivate		30
Module 2 Port 4 FXO	Deactivate		30

2. Configure the table as required. For descriptions of the parameters, see the table below.
3. Click **Submit** to apply your changes.

**Call Forward Table Parameter Description**

Parameter	Description
Forward Type CLI: type [FwdInfo_Type]	<p>Defines the condition upon which the call is forwarded.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Deactivate = (Default) Don't forward incoming calls.</li> <li>▪ <b>[1]</b> On Busy = Forward incoming calls when the port is busy.</li> <li>▪ <b>[2]</b> Unconditional = Always forward incoming calls.</li> <li>▪ <b>[3]</b> No Answer = Forward incoming calls that are not answered within the time specified in the 'Time for No Reply Forward' field.</li> <li>▪ <b>[4]</b> On Busy or No Answer = Forward incoming calls when the port is busy or when calls are not answered within the time specified in the 'Time for No Reply Forward' field.</li> <li>▪ <b>[5]</b> Do Not Disturb = Immediately reject incoming calls.</li> </ul>
Forward to Phone Number CLI: destination [FwdInfo_Destination]	<p>Defines the telephone number or URI (&lt;number&gt;@&lt;IP address&gt;) to where the call is forwarded.</p> <p><b>Note:</b> If this parameter is configured with only a telephone number and a Proxy isn't used, this forwarded-to phone number must be specified in the Outbound IP Routing Table (see 'Configuring Outbound IP Routing Table' on page 321).</p>
Time for No Reply Forward CLI: no-reply-time [FwdInfo_NoReplyTime]	<p>If you have set the 'Forward Type' for this port to <b>No Answer</b>, then configure the number of seconds the device waits before forwarding the call to the specified phone number.</p>

## 31.9 Configuring Caller ID Permissions

The Caller ID Permissions table allows you to enable per port, Caller ID generation for FXS interfaces and Caller ID detection for FXO interfaces.



### Notes:

- If Caller ID permissions is not configured for a port in this table, its Caller ID generation / detection is determined according to the global parameter, 'Enable Call ID' in the Supplementary Services page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **DTMF and Supplementary** > **Supplementary Services**).
- The Caller ID Permissions table can also be configured using the table ini file parameter, EnableCallerID or the CLI command, configure voip > gw analoggw enable-caller-id.

### ➤ To configure Caller ID permissions per port:

1. Open the Caller ID Permissions page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Analog Gateway** > **Caller ID Permissions**).

**Figure 31-9: Caller ID Permissions Page**

Gateway Port	Caller ID
Module 1 Port 1 FXS	Enable ▼
Module 1 Port 2 FXS	Disable ▼
Module 2 Port 1 FXO	▼
Module 2 Port 2 FXO	▼
Module 2 Port 3 FXO	▼
Module 2 Port 4 FXO	▼

2. Configure the table as required. For a description of the parameter, see the table below.
3. Click **Submit** to apply your changes.

**Caller ID Permissions Table Parameter Description**

Parameter	Description
Caller ID CLI: caller-id [EnableCallerId_IsEnabled]	Enables Caller ID generation (FXS) or detection (FXO) per port. <ul style="list-style-type: none"> <li>▪ [0] Disable</li> <li>▪ [1] Enable</li> </ul>

## 31.10 Configuring Call Waiting

The Call Waiting table allows you to enable or disable call waiting per FXS port.



### Notes:

- This page is applicable only to FXS interfaces.
- You can enable or disable call waiting for all the device's ports using the global parameter, 'Enable Call Waiting' in the Supplementary Services page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **DTMF and Supplementary** > **Supplementary Services**).
- The CPT file installed on the device must include a 'call waiting Ringback' tone (caller side) and a 'call waiting' tone (called side, FXS interfaces only).
- The EnableHold parameter must be enabled on both the calling and the called sides.
- For additional call waiting configuration, see the following parameters: FirstCallWaitingToneID (in the CPT file), TimeBeforeWaitingIndication, WaitingBeepDuration, TimeBetweenWaitingIndications, and NumberOfWaitingIndications.
- The Call Waiting table can also be configured using the table ini file parameter, CallWaitingPerPort or CLI command, configure voip > gw analoggw call-waiting.

### ➤ To enable call waiting per port:

1. Open the Call Waiting page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Analog Gateway** > **Call Waiting**).

**Figure 31-10: Call Waiting Page**

Gateway Port	Call Waiting Configuration
Module 1 Port 1 FXS	Enable <input type="button" value="v"/>
Module 1 Port 2 FXS	Enable <input type="button" value="v"/>
Module 2 Port 1 FXO	<input type="button" value="v"/>
Module 2 Port 2 FXO	<input type="button" value="v"/>
Module 2 Port 3 FXO	<input type="button" value="v"/>
Module 2 Port 4 FXO	<input type="button" value="v"/>

2. Configure the table as required. For a description of the parameter, see the table below.
3. Click **Submit** to apply your changes.

### Call Waiting Table Parameter Description

Parameter	Description
Call Waiting Configuration CLI: enable-call-waiting [CallWaitingPerPort_IsEnabled]	<p>Enables call waiting for the port.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable</li> <li>▪ <b>[1]</b> Enable = Enables call waiting for the port. When the device receives a call on a busy port, it responds with a SIP 182 response (not with a 486 busy). The device plays a call waiting indication</li> </ul>

Parameter	Description
	signal. When the device detects a hook-flash from the FXS port, the device switches to the waiting call. The device that initiated the waiting call plays a call waiting ringback tone to the calling party after a 182 response is received.

## 31.11 Rejecting Anonymous Calls

You can configure the device to reject anonymous calls received from the IP and destined for a specific FXS port. This can be configured using the ini file parameter, `RejectAnonymousCallPerPort`. If configured, when an FXS interface receives an anonymous call, the device rejects the call and responds with a SIP 433 (Anonymity Disallowed) response. For a description of the parameter see 'Caller ID Parameters' on page 773.

## 31.12 Configuring FXS Distinctive Ringing and Call Waiting Tones per Source/Destination Number

You can configure a distinctive ringing tone and call waiting tone per calling (source) and/or called (destination) number (or prefix) for IP-to-Tel calls. This feature can be configured per FXS endpoint or for a range of FXS endpoints. Therefore, different tones can be played per FXS endpoint depending on the source and/or destination number of the received call. You can also configure multiple entries with different source and/or destination prefixes and tones for the same FXS port.

Typically, the played ring and/or call waiting tone is indicated in the SIP Alert-info header field of the received INVITE message. If this header is not present in the received INVITE, then this feature is used and the tone played is according to the settings in this table.

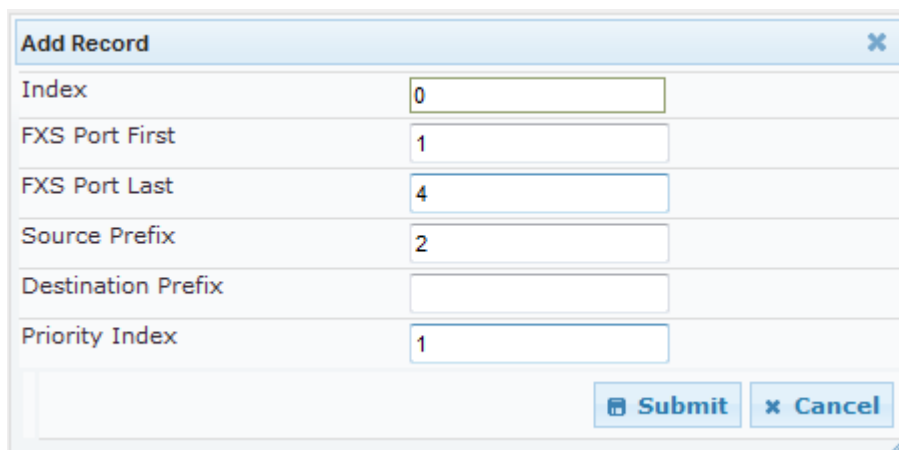


### Notes:

- This page is applicable only to FXS interfaces.
- The Tone Index table can also be configured using the table ini file parameter, `ToneIndex` or CLI command, `configure voip > gw analoggw tone-index`.

- **To configure distinctive ringing and call waiting per FXS port:**
- 1. Open the Tone Index Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Analog Gateway** > **Tone Index**).
- 2. Click the **Add** button; the following dialog box appears:

**Figure 31-11: Tone Index Table Page**



The figure above shows a configuration example for using distinctive ringing and call waiting tones of Index #9 ('Priority Index' 1) in the CPT file for FXS endpoints 1 to 4 when a call is received from a source number with prefix 2.

- 3. Configure the table as required. For a description of the parameters, see the table below.
- 4. Click **Submit** to apply your changes.

**Tone index Table Parameter Description**

Parameter	Description
Index	Defines the table index entry. Up to 50 entries can be defined.
FXS Port First CLI: fxs-port-first [ToneIndex_FXSPort_First]	Defines the first port in the FXS port range.
FXS Port Last CLI: fxs-port-last [ToneIndex_FXSPort_Last]	Defines the last port in the FXS port range.
Source Prefix CLI: src-prefix [ToneIndex_SourcePrefix]	Defines the prefix of the calling number.
Destination Prefix CLI: dst-prefix [ToneIndex_DestinationPrefix]	Defines the prefix of the called number.
Priority Index CLI: priority [ToneIndex_PriorityIndex]	Defines the index of the distinctive ringing and call waiting tones. The call waiting tone index equals to the Priority Index plus the value of the FirstCallWaitingToneID parameter. For example, if you want to use the call waiting tone in the CPT file at Index #9, you need to enter "1" as the Priority Index value and set the FirstCallWaitingToneID parameter to "8". The summation of these values is 9, i.e., index #9. The default is 0.



## 31.13 FXS/FXO Coefficient Types

The FXS Coefficient and FXO Coefficient types used by the device can be one of the following:

- US line type of 600 ohm AC impedance and 40 V RMS ringing voltage for REN = 2
- European standard (TBR21)

These Coefficient types are used to increase return loss and trans-hybrid loss performance for two telephony line type interfaces (US or European). This adaptation is performed by modifying the telephony interface characteristics. This means, for example, that changing impedance matching or hybrid balance doesn't require hardware modifications, so that a single device is able to meet requirements for different markets. The digital design of the filters and gain stages also ensures high reliability, no drifts (over temperature or time) and simple variations between different line types.



The FXS Coefficient types provide best termination and transmission quality adaptation for two FXS line type interfaces. This parameter affects the following AC and DC interface parameters:

- DC (battery) feed characteristics
- AC impedance matching
- Transmit gain
- Receive gain
- Hybrid balance
- Frequency response in transmit and receive direction
- Hook thresholds
- Ringing generation and detection parameters

### ➤ To select the FXO and FXS Coefficient types:

1. Open the Analog Settings page (**Configuration** tab > **VoIP** menu > **Media** > **Analog Settings**). This page includes the Coefficient type parameters, as shown below:

**Figure 31-12: FXS/FXO Coefficient Parameters in Analog Settings Page**

 FXS Coefficient Type	USA	▼
 FXO Coefficient Type	USA	▼

2. From the 'FXS Coefficient Type' drop-down list (FXSCountryCoefficients), select the required FXS Coefficient type.
3. From the 'FXO Coefficient Type' drop-down list (CountryCoefficients), select the required FXO Coefficient type.
4. Click **Submit**.
5. Save your settings to the flash memory ("burn") with a device reset.

## 31.14 FXO Operating Modes

This section provides a description of the device's FXO operating modes:

- For IP-to-Tel calls (see 'FXO Operations for IP-to-Tel Calls' on page [406](#))
- For Tel-to-IP calls (see 'FXO Operations for Tel-to-IP Calls' on page [408](#))
- Call termination on FXO devices (see 'Call Termination on FXO Devices' on page [410](#))

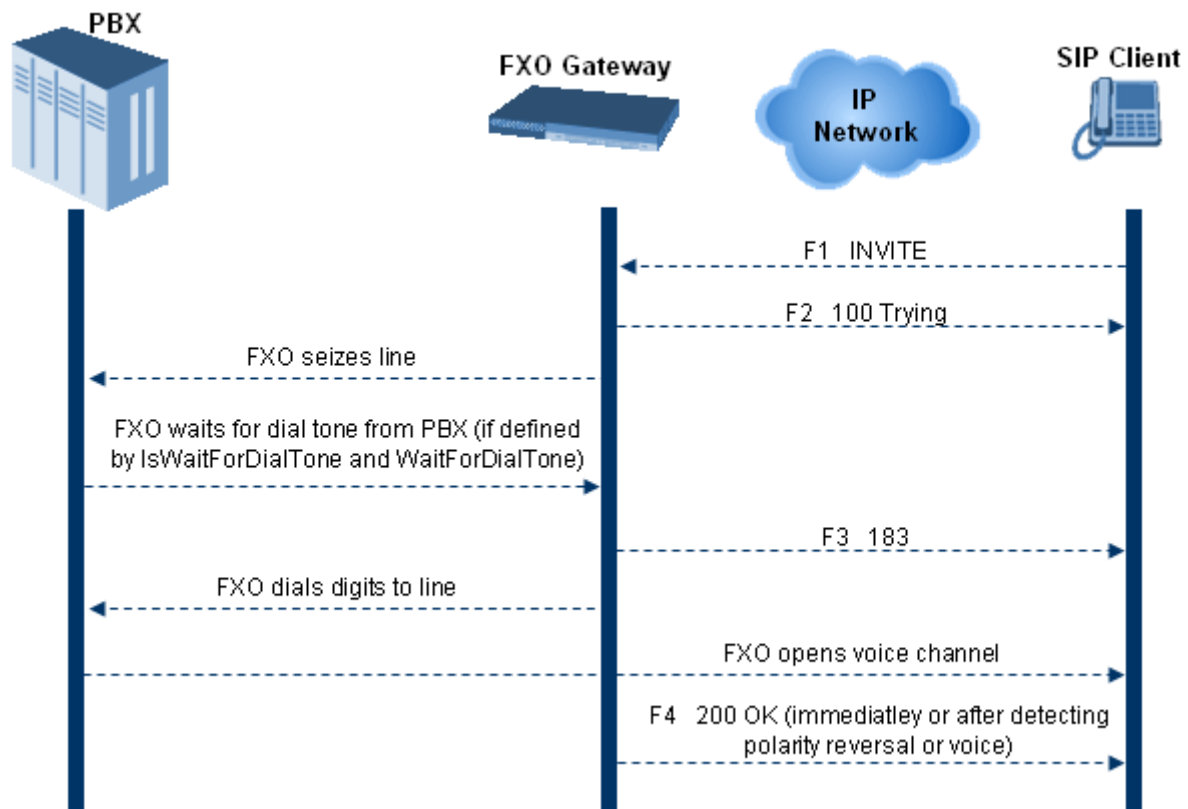
### 31.14.1 FXO Operations for IP-to-Tel Calls

The FXO device provides the following operating modes for IP-to-Tel calls:

- One-stage dialing (see 'One-Stage Dialing' on page 406)
  - Waiting for dial tone (see 'Two-Stage Dialing' on page 407)
  - Time to wait before dialing
  - Answer supervision
- Two-stage dialing (see 'Two-Stage Dialing' on page 407)
- Dialing time: DID wink (see 'DID Wink' on page 407)

#### 31.14.1.1 One-Stage Dialing

One-stage dialing is when the FXO device receives an IP-to-Tel call, off-hooks the PBX line connected to the telephone, and then immediately dials the destination telephone number. In other words, the IP caller doesn't dial the PSTN number upon hearing a dial tone.



One-stage dialing incorporates the following FXO functionality:

- **Waiting for Dial Tone:** Enables the device to dial the digits to the Tel side only after detecting a dial tone from the PBX line. The *ini* file parameter *IsWaitForDialTone* is used to configure this operation.
- **Time to Wait Before Dialing:** Defines the time (in msec) between seizing the FXO line and starting to dial the digits. The *ini* file parameter *WaitForDialTime* is used to configure this operation.



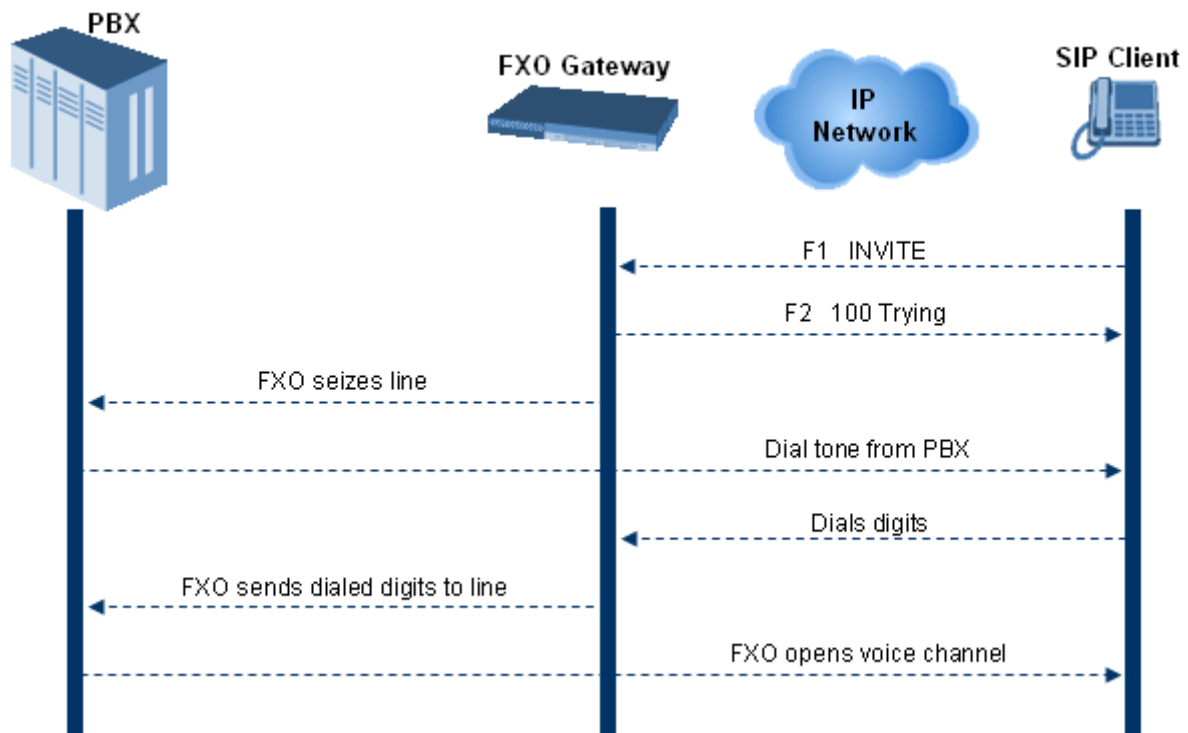
**Note:** The *ini* file parameter *IsWaitForDialTone* must be disabled for this mode.

- **Answer Supervision:** The Answer Supervision feature enables the FXO device to determine when a call is connected, by using one of the following methods:
  - **Polarity Reversal:** the device sends a 200 OK in response to an INVITE only when it detects a polarity reversal.
  - **Voice Detection:** the device sends a 200 OK in response to an INVITE only when it detects the start of speech (fax or modem answer tone) from the Tel side. Note that the IPM detectors must be enabled.

### 31.14.1.2 Two-Stage Dialing

Two-stage dialing is when the IP caller is required to dial twice. The caller initially dials to the FXO device and only after receiving a dial tone from the PBX (via the FXO device), dials the destination telephone number.

**Figure 31-13: Call Flow for Two-Stage Dialing**



Two-stage dialing implements the Dialing Time feature. Dialing Time allows you to define the time that each digit can be separately dialed. By default, the overall dialing time per digit is 200 msec. The longer the telephone number, the greater the dialing time.

The relevant parameters for configuring Dialing Time include the following:

- **DTMFDigitLength (100 msec):** time for generating DTMF tones to the PSTN (PBX) side
- **DTMFInterDigitInterval (100 msec):** time between generated DTMF digits to PSTN (PBX) side

### 31.14.1.3 DID Wink

The device's FXO ports support Direct Inward Dialing (DID). DID is a service offered by telephone companies that enables callers to dial directly to an extension on a PBX without the assistance of an operator or automated call attendant. This service makes use of DID trunks, which forward only the last three to five digits of a phone number to the PBX. If, for

example, a company has a PBX with extensions 555-1000 to 555-1999, and a caller dials 555-1234, the local central office (CO) would forward, for example, only 234 to the PBX. The PBX would then ring extension 234.

DID wink enables the originating end to seize the line by going off-hook. It waits for acknowledgement from the other end before sending digits. This serves as an integrity check that identifies a malfunctioning trunk and allows the network to send a re-order tone to the calling party.

The "start dial" signal is a wink from the PBX to the FXO device. The FXO then sends the last four to five DTMF digits of the called number. The PBX uses these digits to complete the routing directly to an internal station (telephone or equivalent)

- DID Wink can be used for connection to EIA/TIA-464B DID Loop Start lines
- Both FXO (detection) and FXS (generation) are supported

### 31.14.2 FXO Operations for Tel-to-IP Calls

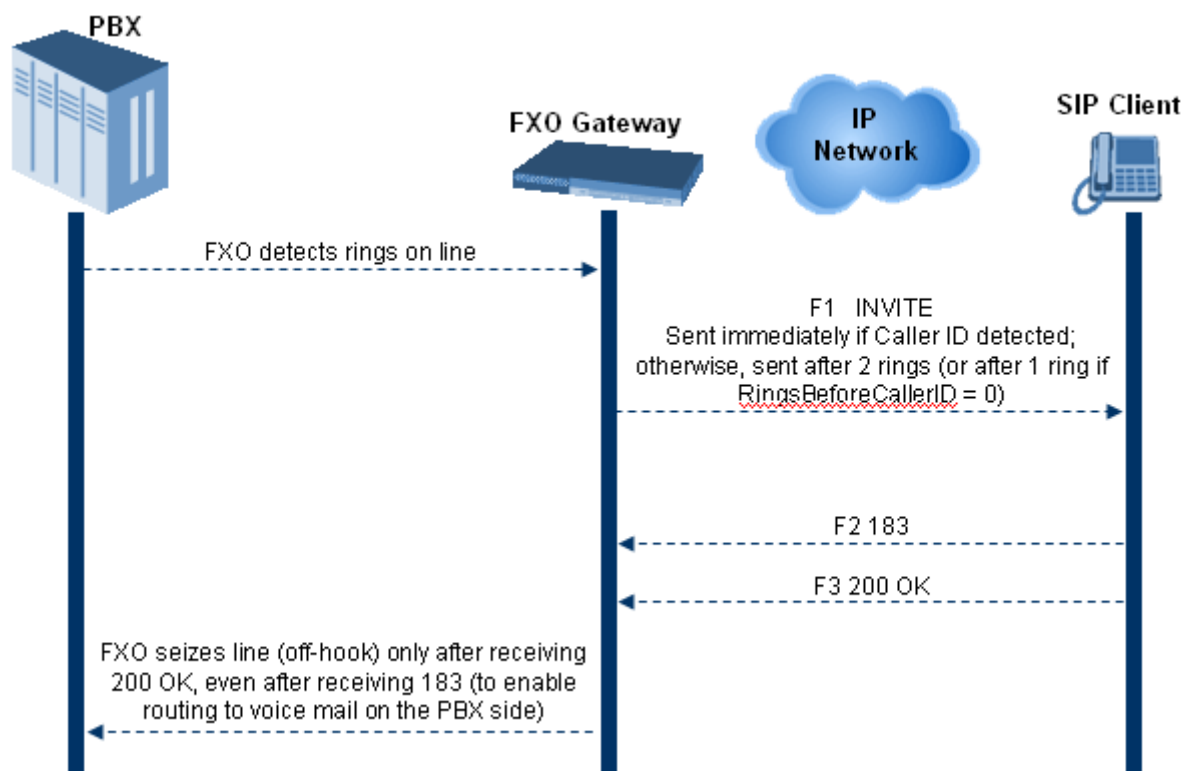
The FXO device provides the following FXO operating modes for Tel-to-IP calls:

- Automatic Dialing (see 'Automatic Dialing' on page 408)
- Collecting Digits Mode (see 'Collecting Digits Mode' on page 409)
- FXO Supplementary Services (see 'FXO Supplementary Services' on page 409)
  - Hold/Transfer Toward the Tel side
  - Hold/Transfer Toward the IP side
  - Blind Transfer to the Tel side

#### 31.14.2.1 Automatic Dialing

Automatic dialing is defined using the Web interface's Automatic Dialing (TargetOfChannel ini file parameter) page, described in see 'Configuring Automatic Dialing' on page 396.

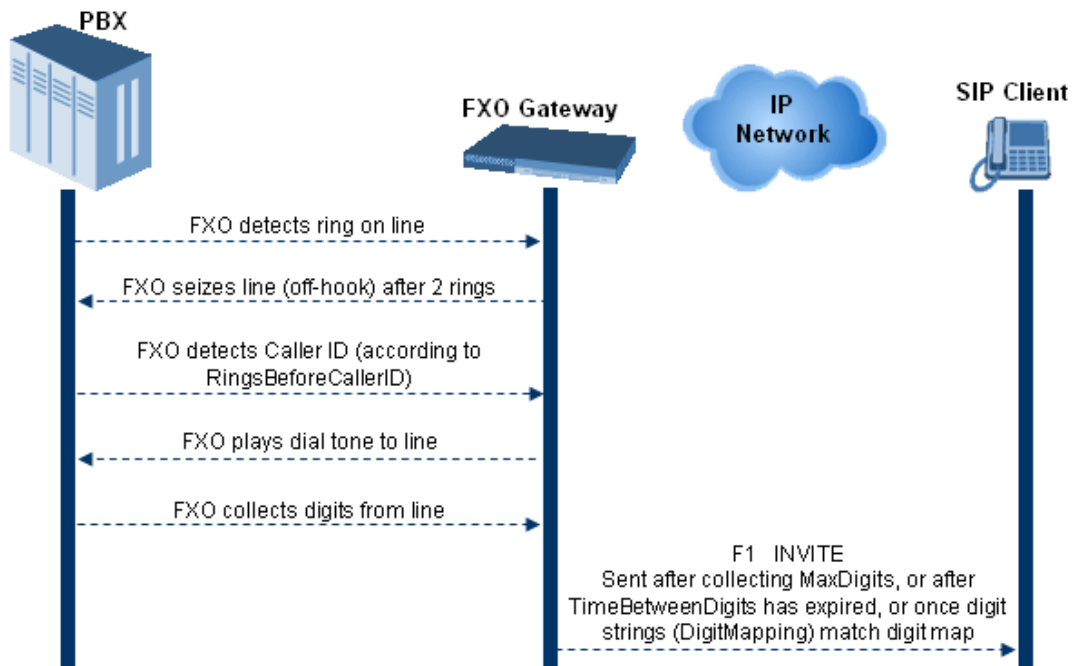
The SIP call flow diagram below illustrates Automatic Dialing.



### 31.14.2.2 Collecting Digits Mode

When automatic dialing is not defined, the device collects the digits. The SIP call flow diagram below illustrates the Collecting Digits Mode.

**Figure 31-14: Call Flow for Collecting Digits Mode**



### 31.14.2.3 FXO Supplementary Services

The FXO supplementary services include the following:

- **Hold / Transfer toward the Tel side:** The *ini* file parameter *LineTransferMode* must be set to 0 (default). If the FXO receives a hook-flash from the IP side (using out-of-band or RFC 2833), the device sends the hook-flash to the Tel side by performing one of the following:

- Performing a hook flash (i.e., on-hook and off-hook)
- Sending a hook-flash code (defined by the *ini* file parameter *HookFlashCode*)

The PBX may generate a dial tone that is sent to the IP, and the IP side may dial digits of a new destination.

- **Blind Transfer to the Tel side:** A blind transfer is one in which the transferring phone connects the caller to a destination line before ringback begins. The *ini* file parameter *LineTransferMode* must be set to 1.

The blind transfer call process is as follows:

- FXO receives a REFER request from the IP side
- FXO sends a hook-flash to the PBX, dials the digits (that are received in the Refer-To header), and then drops the line (on-hook). Note that the time between flash to dial is according to the *WaitForDialTime* parameter.
- PBX performs the transfer internally
- **Hold / Transfer toward the IP side:** The FXO device doesn't initiate hold / transfer as a response to input from the Tel side. If the FXO receives a REFER request (with or without replaces), it generates a new INVITE according to the Refer-To header.

### 31.14.3 Call Termination on FXO Devices

This section describes the device's call termination capabilities for its FXO interfaces:

- Calls terminated by a PBX (see 'Call Termination by PBX' on page 410)
- Calls terminated before call establishment (see 'Call Termination before Call Establishment' on page 411)
- Ring detection timeout (see 'Ring Detection Timeout' on page 411)

#### 31.14.3.1 Calls Termination by PBX

The FXO device supports various methods for identifying when a call has been terminated by the PBX.

The PBX doesn't disconnect calls, but instead signals to the device that the call has been disconnected using one of the following methods:

- **Detection of polarity reversal/current disconnect:** The call is immediately disconnected after polarity reversal or current disconnect is detected on the Tel side (assuming the PBX/CO generates this signal). This is the recommended method.

Relevant parameters: EnableReversalPolarity, EnableCurrentDisconnect, CurrentDisconnectDuration, CurrentDisconnectDefaultThreshold, and TimeToSampleAnalogLineVoltage.

- **Detection of Reorder, Busy, Dial, and Special Information Tone (SIT) tones:** The call is immediately disconnected after a Reorder, Busy, Dial, or SIT tone is detected on the Tel side (assuming the PBX / CO generates this tone). This method requires the correct tone frequencies and cadence to be defined in the Call Progress Tones file. If these frequencies are unknown, define them in the CPT file. The tone produced by the PBX / CO must be recorded and its frequencies analyzed. Adding a reorder tone to the CPT file can be done using AudioCodes CPTWizard utility (refer to the *CPTWizard Utility User's Guide*). This method is slightly less reliable than the previous one. You can use the CPTWizard to analyze Call Progress Tones generated by any PBX or telephone network.

Relevant parameters: DisconnectOnBusyTone and DisconnectOnDialTone.

- **Detection of silence:** The call is disconnected after silence is detected on both call directions for a specific (configurable) amount of time. The call isn't disconnected immediately; therefore, this method should only be used as a backup option.

Relevant parameters: EnableSilenceDisconnect and FarEndDisconnectSilencePeriod.

- **Special DTMF code:** A digit pattern that when received from the Tel side, indicates to the device to disconnect the call.

Relevant *ini* file parameter: TelDisconnectCode.

- **Interruption of RTP stream:** Relevant parameters: BrokenConnectionEventTimeout and DisconnectOnBrokenConnection.



**Note:** This method operates correctly only if silence suppression is not used.

- **Protocol-based termination of the call from the IP side**



**Note:** The implemented disconnect method must be supported by the CO or PBX.

### 31.14.3.2 Call Termination before Call Establishment

The device supports the following call termination methods before a call is established:

- **Call termination upon receipt of SIP error response (in Automatic Dialing mode):**  
By default, when the FXO device operates in Automatic Dialing mode, there is no method to inform the PBX if a Tel-to-IP call has failed (SIP error response - 4xx, 5xx or 6xx - is received). The reason is that the FXO device does not seize the line until a SIP 200 OK response is received. Use the `FXOAutoDialPlayBusyTone` parameter to allow the device to play a busy / reorder tone to the PSTN line if a SIP error response is received. The FXO device seizes the line (off-hook) for the duration defined by the `TimeForReorderTone` parameter. After playing the tone, the line is released (on-hook).
- **Call termination after caller (PBX) on-hooks phone (Ring Detection Timeout feature):** This method operates in one of the following manners:
  - **Automatic Dialing is enabled:** if the remote IP party doesn't answer the call and the ringing signal (from the PBX) stops for a user-defined time (configured by the parameter `FXOBetweenRingTime`), the FXO device releases the IP call.
  - **No automatic dialing and Caller ID is enabled:** the device seizes the line after detection of the second ring signal (allowing detection of caller ID sent between the first and the second rings). If the second ring signal is not received within this timeout, the device doesn't initiate a call to IP.

### 31.14.3.3 Ring Detection Timeout

The operation of Ring Detection Timeout depends on the following:

- **Automatic dialing is disabled and Caller ID is enabled:** if the second ring signal is not received for a user-defined time (using the parameter `FXOBetweenRingTime`), the FXO device doesn't initiate a call to the IP.
- **Automatic dialing is enabled:** if the remote party doesn't answer the call and the ringing signal stops for a user-defined time (using the parameter `FXOBetweenRingTime`), the FXO device releases the IP call.

Ring Detection Timeout supports full ring cycle of ring on and ring off (from ring start to ring start).

## 31.15 Remote PBX Extension between FXO and FXS Devices

Remote PBX extension offers a company the capability of extending the "power" of its local PBX by allowing remote phones (remote offices) to connect to the company's PBX over the IP network (instead of via PSTN). This is as if the remote office is located in the head office (where the PBX is installed). PBX extensions are connected through FXO ports to the IP network, instead of being connected to individual telephone stations. At the remote office, FXS units connect analog phones to the same IP network. To produce full transparency, each FXO port is mapped to an FXS port (i.e., one-to-one mapping). This allows individual extensions to be extended to remote locations. To call a remote office worker, a PBX user or a PSTN caller simply dials the PBX extension that is mapped to the remote FXS port.

This section provides an example on how to implement a remote telephone extension through the IP network, using FXO and FXS interfaces. In this configuration, the FXO device routes calls received from the PBX to the 'Remote PBX Extension' connected to the FXS device. The routing is transparent as if the telephone connected to the FXS device is directly connected to the PBX.

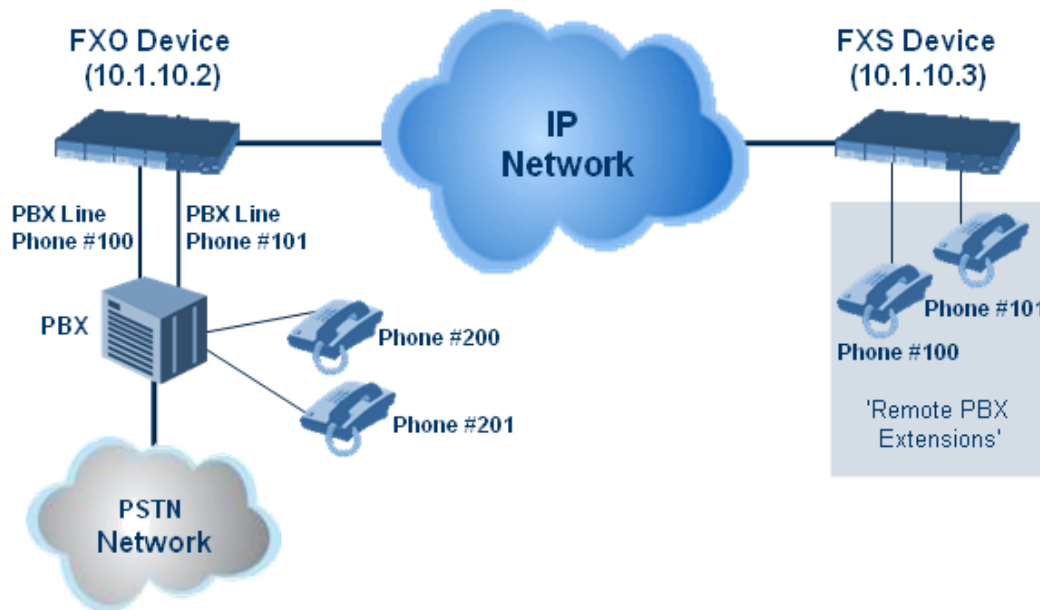
The following is required:

- FXO interfaces with ports connected directly to the PBX lines (shown in the figure



below)

- FXS interfaces for the 'remote PBX extension'
- Analog phones (POTS)
- PBX (one or more PBX loop start lines)
- LAN network



### 31.15.1 Dialing from Remote Extension (Phone at FXS)

The procedure below describes how to dial from the 'remote PBX extension' (i.e., phone connected to the FXS interface).

➤ **To make a call from the FXS interface:**

1. Off-hook the phone and wait for the dial tone from the PBX. This is as if the phone is connected directly to the PBX. The FXS and FXO interfaces establish a voice path connection from the phone to the PBX immediately after the phone is off-hooked.
2. Dial the destination number (e.g., phone number 201). The DTMF digits are sent over IP directly to the PBX. All the audible tones are generated from the PBX (such as ringback, busy, or fast busy tones). One-to-one mapping occurs between the FXS ports and PBX lines.
3. The call disconnects when the phone connected to the FXS goes on-hook.

### 31.15.2 Dialing from PBX Line or PSTN

The procedure below describes how to dial from a PBX line (i.e., from a telephone directly connected to the PBX) or from the PSTN to the 'remote PBX extension' (i.e., telephone connected to the FXS interface).

➤ **To dial from a telephone directly connected to the PBX or from the PSTN:**

- Dial the PBX subscriber number (e.g., phone number 101) in the same way as if the user's phone was connected directly to the PBX. As soon as the PBX rings the FXO device, the ring signal is 'sent' to the phone connected to the FXS device. Once the phone connected to the FXS device is off-hooked, the FXO device seizes the PBX line and the voice path is established between the phone and PBX.



There is one-to-one mapping between PBX lines and FXS device ports. Each PBX line is routed to the same phone (connected to the FXS device). The call disconnects when the phone connected to the FXS device is on-hooked.

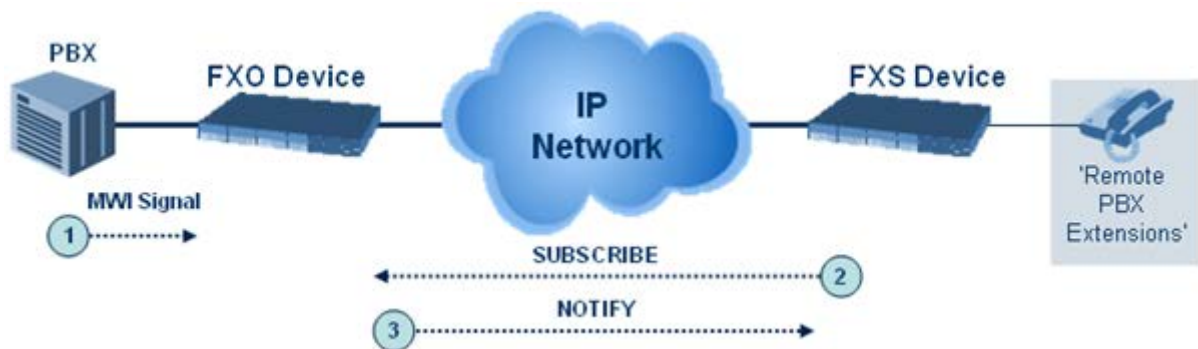
### 31.15.3 Message Waiting Indication for Remote Extensions

The device supports the relaying of Message Waiting Indications (MWI) for remote extensions (and voice mail applications). Instead of subscribing to an MWI server to receive notifications of pending messages, the FXO device receives subscriptions from the remote FXS device and notifies the appropriate extension when messages (and the number of messages) are pending.

The FXO device detects an MWI message from the Tel (PBX) side using any one of the following methods:

- 100 VDC (sent by the PBX to activate the phone's lamp)
- Stutter dial tone from the PBX
- MWI display signal (according to the parameter CallerIDType)

Upon detection of an MWI message, the FXO device sends a SIP NOTIFY message to the IP side. When receiving this NOTIFY message, the remote FXS device generates an MWI signal toward its Tel side.



### 31.15.4 Call Waiting for Remote Extensions

When the FXO device detects a Call Waiting indication (FSK data of the Caller Id - CallerIDType2) from the PBX, it sends a proprietary INFO message, which includes the caller identification to the FXS device. Once the FXS device receives this INFO message, it plays a call waiting tone and sends the caller ID to the relevant port for display. The remote extension connected to the FXS device can toggle between calls using the Hook Flash button.



### 31.15.5 FXS Gateway Configuration

The procedure below describes how to configure the FXS interface (at the 'remote PBX extension').

➤ **To configure the FXS interface:**

1. In the Trunk Group Table page (see , assign the phone numbers 100 to 104 to the device's endpoints.

**Figure 31-15: Assigning Phone Numbers to FXS Endpoints**

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID
1	Module 3 FXS	1	1	1-4	100	0

2. In the Automatic Dialing page (see 'Configuring Automatic Dialing' on page 396), enter the phone numbers of the FXO device in the 'Destination Phone Number' fields. When a phone connected to Port #1 off-hooks, the FXS device automatically dials the number '200'.

**Figure 31-16: Automatic Dialing for FXS Ports**

Gateway Port	Destination Phone Number	Auto Dial Status
Module 3 Port 1 FXS	200	Enable
Module 3 Port 2 FXS	201	Enable
Module 3 Port 3 FXS	202	Enable
Module 3 Port 4 FXS	203	Enable

3. In the Outbound IP Routing Table page (see 'Configuring Outbound IP Routing Table' on page 321), enter 20 for the destination phone prefix, and 10.1.10.2 for the IP address of the FXO device.

	Src. Host Prefix	Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address
1				20	*	10.1.10.2



**Note:** For the transfer to function in remote PBX extensions, Hold must be disabled at the FXS device (i.e., Enable Hold = 0) and hook-flash must be transferred from the FXS to the FXO (HookFlashOption = 4).

### 31.15.6 FXO Gateway Configuration

The procedure below describes how to configure the FXO interface (to which the PBX is directly connected).

➤ **To configure the FXO interface:**

4. In the Trunk Group Table page (see , assign the phone numbers 200 to 204 to the device's FXO endpoints.

**Figure 31-17: Assigning Phone Numbers to FXO Ports**

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number
1	Module 3 FXO ▼	▼	▼	1-4	200

5. In the Automatic Dialing page, enter the phone numbers of the FXS device in the 'Destination Phone Number' fields. When a ringing signal is detected at Port #1, the FXO device automatically dials the number '100'.

**Figure 31-18: FXO Automatic Dialing Configuration**

Gateway Port	Destination Phone Number	Auto Dial Status
Module 3 Port 1 FXO	100	Enable ▼
Module 3 Port 2 FXO	101	Enable ▼
Module 3 Port 3 FXO	102	Enable ▼
Module 3 Port 4 FXO	103	Enable ▼

6. In the Outbound IP Routing Table page, enter 10 in the 'Destination Phone Prefix' field, and the IP address of the FXS device (10.1.10.3) in the field 'IP Address'.

**Figure 31-19: FXO Tel-to-IP Routing Configuration**

	Dest. Phone Prefix	Source Phone Prefix	- >	Dest. IP Address
1	10	*		10.1.10.3

7. In the FXO Settings page (see 'Configuring FXO Parameters' on page 394), set the parameter 'Dialing Mode' to **Two Stages** (IsTwoStageDial = 1).

## Reader's Notes

# Part VI

## Session Border Controller Application



## 32 SBC Overview

This section provides a detailed description of the device's SBC application.

**Notes:**

- For guidelines on how to deploy your E-SBC device based on network topology, refer to the *SBC Design Guide* document.
- For SBC functionality, the Software License Key installed on the device must include the SBC feature.

The SBC application supports the following main features:

- NAT traversal: The device supports NAT traversal, allowing, for example, communication with ITSPs with globally unique IP addresses, for LAN-to-WAN VoIP signaling (and bearer), using two independent legs. This also enables communication for "far-end" users located behind a NAT on the WAN. The device supports this by:
  - Continually registering far-end users in its dynamic database.
  - Maintaining remote NAT binding state by frequent registrations, thereby, off-loading far-end registrations from the LAN IP PBX.
  - Using Symmetric RTP (RFC 4961) to overcome bearer NAT traversal.
- VoIP firewall and security for signaling and media:
  - SIP signaling:
    - ◆ Deep and stateful inspection of all SIP signaling packets.
    - ◆ SIP dialog initiations may be rejected based on values of incoming SIP INVITE message and other Layer-3 characteristics.
    - ◆ Packets not belonging to an authorized SIP dialog are discarded.
  - RTP:
    - ◆ Opening pinholes (ports) in the device's firewall based on Offer-Answer SDP negotiations.
    - ◆ Deep packet inspection of all RTP packets.
    - ◆ Late rouge detection - if a SIP session was gracefully terminated and someone tries to "ride on it" with rouge traffic from the already terminated RTP and SIP context, the VoIP Firewall prevents this from occurring.
    - ◆ Disconnects call (after user-defined time) if RTP connection is broken.
    - ◆ Black/White lists for both Layer-3 firewall and SIP classification.
- Topology hiding: The device intrinsically supports topology hiding, limiting the amount of topology information displayed to external parties. For example, IP addresses of ITSPs' equipment (e.g. proxies, gateways, and application servers) can be hidden from outside parties. The device's topology hiding is provided by implementing back-to-back user agent (B2BUA) leg routing:
  - Strips all incoming SIP Via header fields and creates a new Via value for the outgoing message.
  - Each leg has its own Route/Record Route set.
  - Modifies SIP To, From, and Request-URI host names (must be configured using the Message Manipulations table).
  - Generates a new SIP Call-ID header value (different between legs).
  - Changes the SIP Contact header to the device's own address.
  - Layer-3 topology hiding by modifying source IP address in the SIP IP header.
- SIP normalization: The device supports SIP normalization, whereby the SBC

application can overcome interoperability problems between SIP user agents. This is achieved by the following:

- Manipulation of SIP URI user and host parts.
- Connection to ITSP SIP trunks on behalf of an IP-PBX - the device can register and utilize user and password to authenticate for the IP-PBX.
- Survivability:
  - Routing calls to alternative routes such as the PSTN.
  - Routing calls between user agents in the local network using a dynamic database (built according to registrations of SIP user agents).
- Routing:
  - IP-to-IP routing translations of SIP, UDP, TCP, TLS (when extensive transcoding is not required).
  - Load balancing and redundancy of SIP servers.
  - Routing according to Request-URI\Specific IP address\Proxy\FQDN.
  - Alternative routing.
  - Routing between different Layer-3 networks (e.g., LAN and WAN).
- Load balancing\redundancy of SIP servers.
- ITSP accounts.
- SIP URI user and host name manipulations.
- Coder transcoding.

## 32.1 SIP Network Definitions

The device's SBC application can implement multiple SIP signaling and RTP (media) interfaces.

## 32.2 SIP Dialog Initiation Process

The device's SIP dialog initiation process concerns all incoming SIP dialog initiation requests. This includes SIP methods such as INVITE, SUBSCRIBE, OPTIONS, REFER, INFO, UNSOLICITED NOTIFY, MESSAGE, and REGISTER.

The SIP dialog initiation process consists of the following stages:

1. **Determining source and destination URL:** The SIP protocol has more than one URL in a dialog-establishing request that may represent the source and destination URLs. When handling an incoming request, the device uses specific SIP headers for obtaining the source and destination URLs. Once these URLs are determined, their user and host parts are used as input for the classification process, message manipulation, and call routing.
  - **All SIP requests (e.g., INVITE) except REGISTER dialogs:**
    - ◆ Source URL: The source URL is obtained from the SIP header according to the following logic:
      - ✓ The source URL is obtained from the From header.
      - ✓ If the From header contains the value 'Anonymous', the source URL is obtained from the P-Preferred-Identity header.
      - ✓ If the P-Preferred-Identity header does not exist, the source URL is obtained from the P-Asserted-Identity header.
    - ◆ Destination URL: The destination URL is obtained from the Request-URI.
  - **REGISTER dialogs:**
    - ◆ Source URL: The source URL is obtained from the To header.



- ◆ Destination URL: The destination URL is obtained from the Request-URI.

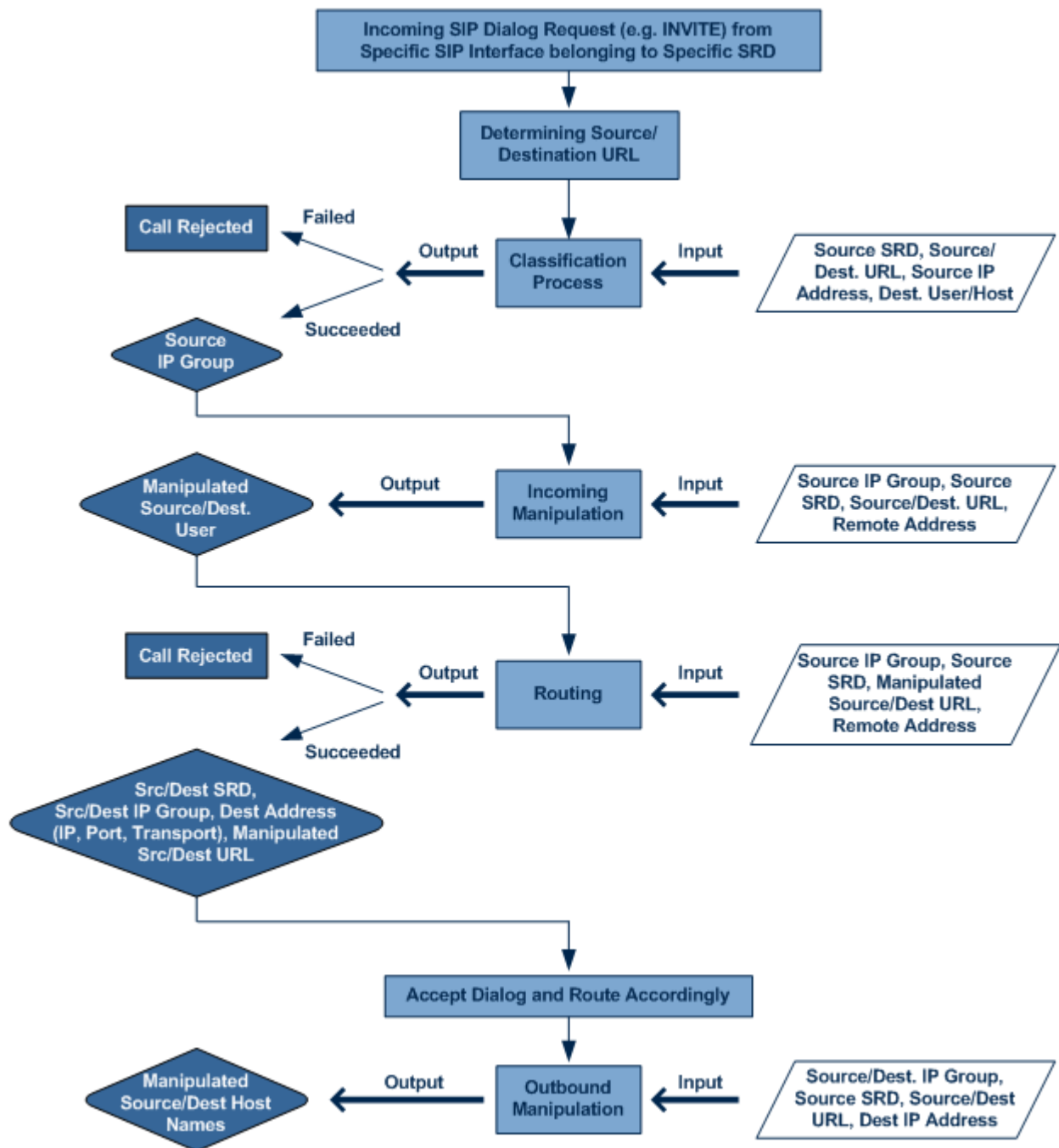


**Note:** You can determine the SIP header from where the device obtains the source URL in the incoming SIP request. This is done in the IP Group table using the 'Source URI Input' parameter.

- 2. Classifying incoming SIP dialog-initiating requests to a source IP Group:** The classification identifies the incoming SIP dialog request as belonging to a specific IP Group (from where the SIP dialog request originated). For more information, see 'Configuring Classification Rules' on page 456.
- 3. SBC IP-to-IP routing:** The device routes the call to a destination that can be configured to one of the following:
  - Registered user Contact listed in the device's database (only for User-type IP Groups).
  - IP Group - the destination is the address configured for the Proxy Set associated with the IP Group (allows redundancy/load balancing).
  - Specified destination address (can be based on IP address, host name, port, transport type, and/or SRD). Routing to a host name can be resolved using NAPTR/SRV/A-Record.
  - Request-URI of incoming SIP dialog initiating requests.
  - ENUM query.
  - Hunt Group - used for call survivability.
  - IP address (in dotted-decimal notation or FQDN - NAPTR/SRV/A-Record resolutions) according to a specified Dial Plan index listed in the loaded Dial Plan file.
  - LDAP server or LDAP query result.For more information, see 'Configuring SBC IP-to-IP Routing' on page 462.
- 4. Manipulating SIP URI user part (source and destination) of inbound and/or outbound SIP dialog requests:** You can configure rules for manipulating the SIP URI user part (source and destination) on the inbound and/or outbound leg. For more information, see 'SBC Manipulations' on page 469.
- 5. SIP message manipulations:** You can configure SIP message manipulation rules that can add, remove, and/or modify SIP headers and parameters. For more information, see 'Configuring SIP Message Manipulation' on page 226.

The flowchart below illustrates the SBC process:

**Figure 32-1: Routing Process**



## 32.3 User Registration and Internal Database

To allow registrations to traverse the SBC, the device must be configured with at least one User-type IP Group. These IP Groups represent a group of user agents that share the following characteristics:

- Perform registrations and share the same serving proxy/registrar
- Possess identical SIP and media behavior
- Reside on the same Layer-3 network and are associated with the same SRD

Typically, the device is configured as the user agent's outbound proxy and the device is configured (using the IP-to-IP Routing table) to route requests received from this IP Group to the serving proxy and vice versa. Survivability can be achieved using the alternative routing feature.

### 32.3.1 Initial Registration Request Processing

Registration requests have different processing policies than other SIP methods:

1. Determining source and destination URL's:
  - The source URL is obtained from the To header
  - The destination URL is obtained from the Request URI
2. Classification: The REGISTER classification process is the same as the general classification process (described in previous sections). The source IP Group must be of type User. If classification fails or the source IP Group is not of type User, the registration is rejected.
3. Routing: The REGISTER routing is performed using the IP-to-IP Routing table:
  - The destination type can be an IP Group, specific IP address, Request-URI, or ENUM query (can also use DNS queries).
  - If the destination is a User-type IP Group, then the registration is not be forwarded. Instead, the device accepts (replies with 200 OK response) or rejects (Reply with 4xx) the request according to the user group policy.
4. Internal registration database: If the source IP Group is of type User and registration succeeds (replied with 200 OK by the IP-PBX), then the device adds a record to its database that identified the specific contact of this specific user (AOR). This record is used later to route requests to this specific user (either in normal or in survivability modes).
5. Alternative Routing: Alternative routing can be configured in the IP-to-IP Routing table for REGISTER requests.
6. Inbound Manipulation: The SBC record in the device's database includes the Contact header. Every REGISTER request is added to the database before manipulation, allowing correct user identification in the SBC Classification process for the next received request.
7. Session Admission Control: Applies various limitations on incoming and outgoing REGISTER requests. For example, limiting REGISTER requests from a certain IP Group/SRD. Note that this limitation is only for concurrent register dialogs and not concurrent registrations in the internal database.
8. The device can retain the original value of the SIP Expires header received from the user or proxy, in the outgoing REGISTER message. This feature also applies when the device is in "survivability" state (i.e., REGISTER requests cannot be forwarded to the proxy and is terminated by the device). This is configured by the `SBCUserRegistrationTime`, `SBCProxyRegistrationTime`, and `SBCSurvivabilityRegistrationTime` parameters.
9. By default, the Contact of the outgoing REGISTER is populated with a unique Contact generated by the device and associated with this specific registration. Alternatively, the original user can be retained in the Contact and used in the outgoing REGISTER request (using the `SBCKeepContactUserinRegister` parameter).

### 32.3.2 Internal Database

The device manages a dynamic database that is updated according to registration requests that traverse the SBC. Each database entry represents a binding between an AOR and one or more contact. Database bindings are added upon successful registration

responses. For specific registrations, the AOR is obtained from the SIP To header and the contact is taken from the SIP Contact header.

Database bindings are removed in the following cases:

- Successful de-registration responses (REGISTER with Expires header that equals zero)
- Registration failure responses
- Timeout of the Expires header value (in scenarios where the user agent did not send a refresh registration request)

The database has the following limitations:

- Maximum of five contacts per AOR
- The same contact cannot belong to more than one AOR
- Contacts with identical URIs and different ports and transport types are not supported (same key is created)
- Multiple contacts in a single REGISTER is not supported
- One database is shared between all User-type IP Groups

### 32.3.3 Routing using Internal Database

Typically, routing using the database is applicable to all method types other than registrations. To route to a registered user (using the internal dynamic database), the following steps must be taken:

1. An IP-to-IP Routing rule with the desired input parameters (matching characteristics) and the destination type as IP Group (operation rule).
2. The destination IP Group must be of type User.
3. To find a match for these specific rules, the device attempts to locate a match between the incoming Request-URI and (according to the description order):
  - a. Unique contact - the Contact generated by the SBC and sent in the initial registration request to the serving proxy
  - b. Registered AOR - the AOR of the incoming REGISTER request
  - c. Registered contact - the Contact of the incoming REGISTER request

If registrations are destined to the database (using the above rules), the device does not attempt to find a database match, but instead replies with 200 OK (used for Survivability). Once a match is found, the request is routed either to the contact received in the initial registration or (if the device identifies that the user agent is behind a NAT) to the source IP address of the initial registration.

### 32.3.4 Registration Refreshes

Registration refreshes are incoming REGISTER requests that are associated with a specific registered user. The association is performed by searching the internal registration database. These refreshes are routed to the serving proxy only if the serving proxy Expires time is about to expire; otherwise, the device responds with a 200 OK without routing the REGISTER. Each such refreshes also refresh the internal timer time set on the device for this specific registration.

### 32.3.5 Notification of Expired User Registration to SIP Proxy / Registrar

The device automatically notifies SIP Proxy / Registrar servers of users registered in the device's database whose registration timeout has expired. When a user's registration timer expires, the device removes the user record from its Registration database and sends an unregister notification (REGISTER message with the Expires header set to 0) to the Proxy/Registrar.

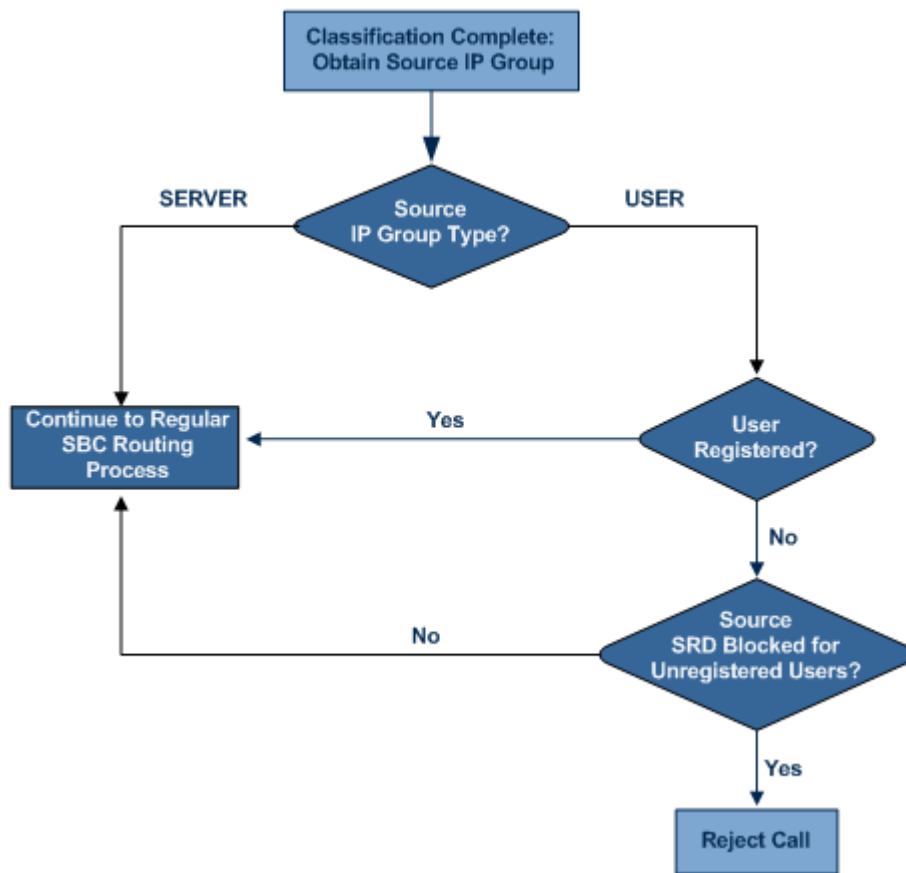
This feature is enabled only if a REGISTER message is sent to an IP Group destination type, configured in the IP-to-IP Routing table.

### 32.3.6 Registration Restriction Control

The device provides flexibility in controlling user registration:

- **Limiting Number of Registrations per Source SRD and/or IP Group:** You can limit the number of users that can register with the device. This limitation can be applied per source IP Group and/or SRD. By default, no limitation exists for registered users. This is configured using the parameters SRD or IPGroup.
- **Blocking Incoming Calls from Unregistered Users:** You can block incoming calls (INVITE requests) from unregistered users (pertaining to User-type IP Groups). By default, calls from unregistered users are not blocked. This is configured using the parameter SRD. The flowchart below depicts the process for blocking unregistered users. When the call is rejected, the device sends a SIP 500 "Server Internal Error" response to the remote end.

Figure 32-2: Blocking Incoming Calls from Unregistered Users



## 32.4 SBC Media Handling

Media behavior includes anything related to the establishment, management and termination of media sessions within the SIP protocol. Media sessions are created using the SIP "offer"/"answer" mechanism. If successful, the result is a bi-directional media (RTP) flow (e.g. audio, fax, modem, DTMF). Each offer/answer may create more than one media session of different types (e.g. audio and fax). In a SIP dialog, multiple offer/answer transactions may occur, each may change the media sessions characteristics (e.g. IP

address, port, coders, media types, and RTP mode). The media capabilities exchanged in an offer/answer transaction include the following:

- Media types (Audio, Secure Audio, Video, Fax, Text...)
- IP addresses and ports of the media flow
- Media flow mode (send receive, receive only, send only, inactive)
- Media coders (coders and their characteristics used in each media flow)
- Other (standard or proprietary) media and session characteristics

Even though the device usually does not change the negotiated media capabilities (mainly performed by the remote user agents), it does examine the media exchange to control negotiated media types (if necessary) and to know how to open the RTP media channels (IP addresses, coder type, payload type etc.). The device forwards multiple video streams and text, as is.

The device interworks (normalization) the media (RTP-to-RTP, SRTP-to-RTP, and SRTP-to-SRTP) between its SBC legs. It "re-builds" specific fields in the RTP header when forwarding media packets. The main fields include the sequence number, SSRC, and timestamp.

The device is aware and sometimes active in the offer/answer process due to the following:

- NAT traversal: the device changes the SDP address to be its own address, thereby, resolving NAT problems.
- Firewall and security:
  - RTP pin holes - only RTP packets related to a successful offer/answer negotiation traverse the device: When the device initializes, there are no RTP pin holes opened, this means that each RTP/RTCP packets destined to the device are discarded. Once an offer/answer transaction ends successfully, an RTP pin hole is opened and RTP/RTCP flows between the two remote user agents. Once a pin hole is opened, the payload type and RTP header version is validated for each packet. RTP pin holes close if one of the associated SIP dialogs is closed (may also be due to broken connection).
  - Late rogue detection - once a dialog is disconnected, the related pin holes also disconnect.
  - Deep Packet inspection of the RTP that flows through the opened pin holes.
- Adding of media functionality to SIP user agents:
  - Transcoding (for a description on the transcoding modes, see 'Transcoding Modes' on page 431)
  - Broken connection

According to the above functionalities, the call can be configured to operate in one of the following modes:

- **Media Anchoring without Transcoding (Transparent):** RTP traverses the device with minimal RTP packet changes (no DSP resources needed). This is typically used to solve NAT, firewall, and security issues. In this mode, all the "audio" coders in the received offer are included in the SBC outgoing offer. The Coder Table configuration has no effect on the coders in the outgoing offer. For more information, see 'Media Anchoring without Transcoding (Transparent)' on page 427.
- **Media Anchoring with Transcoding:** RTP traverses the device and each leg uses a different coder or coder parameters (DSP resources are required). For more information, see 'Media Anchoring with Transcoding' on page 427.
- **No Media Anchoring:** The RTP packet flow does not traverse the device. Instead, the two SIP UA's establish a direct RTP/SRTP flow between one another (see 'No Media Anchoring' on page 429).



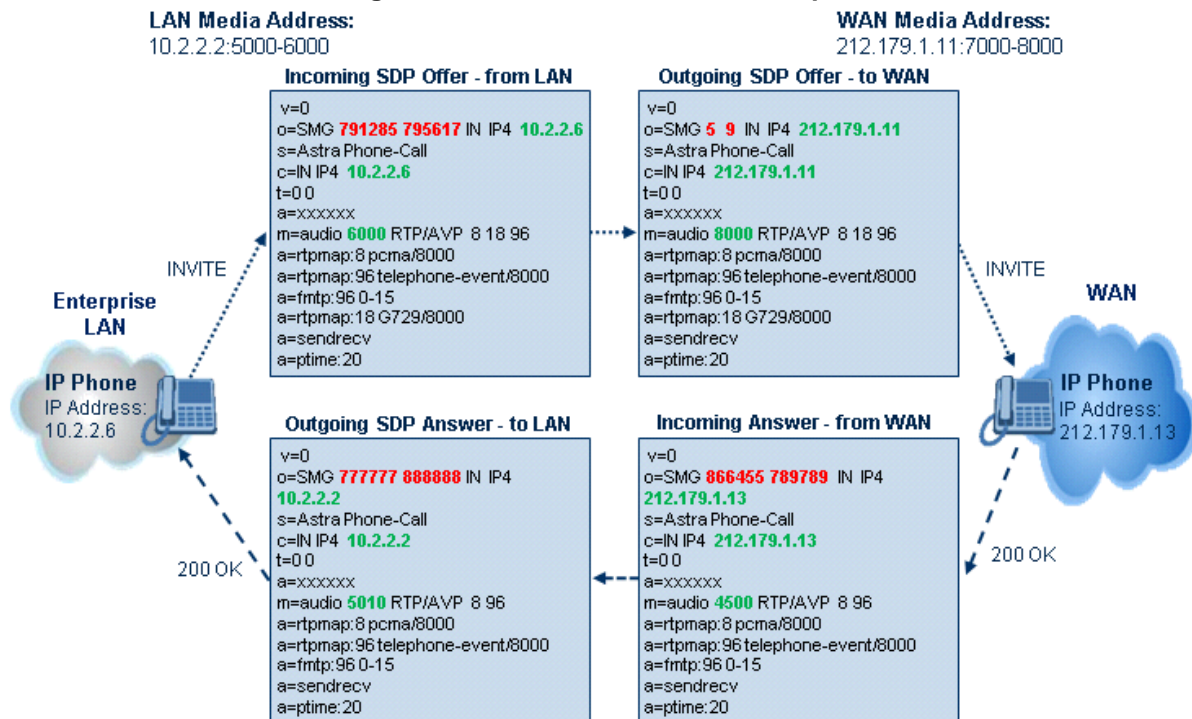
### 32.4.1 Media Anchoring without Transcoding (Transparent)

To direct the RTP to flow through the device (for NAT traversal, firewall and security), all IP address fields in the SDP are modified:

- Origin: IP address, session and version id
- Session connection attribute ('c=' field)
- Media connection attribute ('c=' field)
- Media port number
- RTCP media attribute IP address and port

Each SBC leg allocates and uses the device's local ports (e.g., for RTP/RTCP/fax). The local ports are allocated from a Media Realm associated with each leg. The legs are associated with a Media Realm as follows: If the leg's IP Group is configured with a Media Realm, then this is the associated Media Realm; otherwise, the leg's SRD Media Realm is the associated one. The figure below illustrates an example of SDP handling for a call between a LAN IP Phone 10.2.2.6 and a remote IP Phone 212.179.1.13 on the WAN.

Figure 32-3: SDP Offer/Answer Example



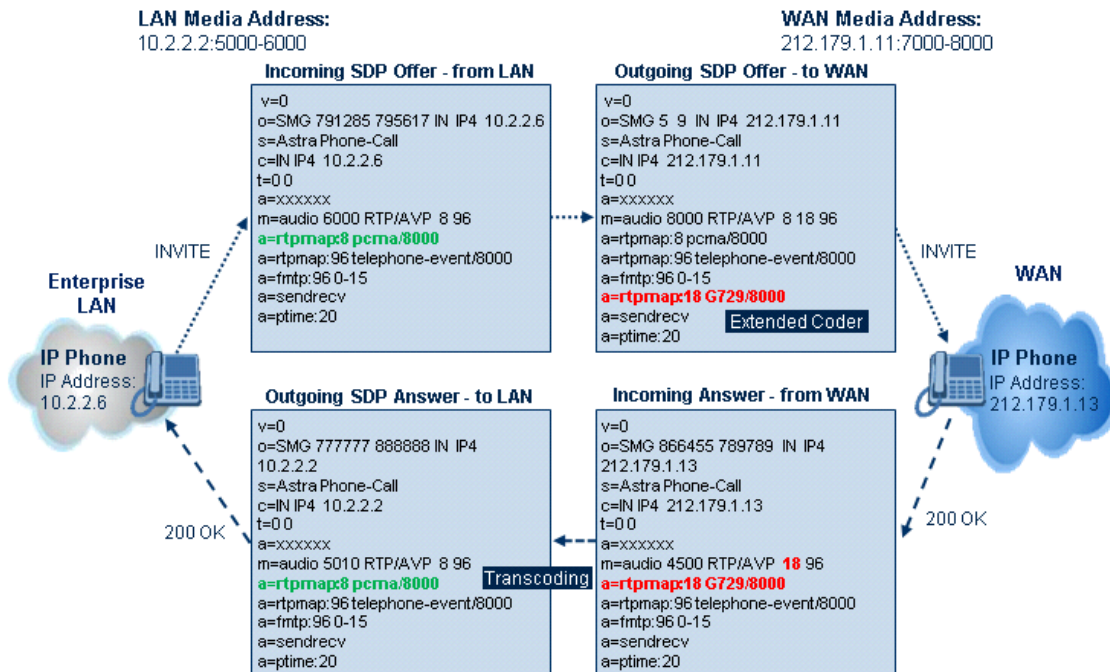
### 32.4.2 Media Anchoring with Transcoding

The device performs transcoding when there are no common coders between the two user agents (i.e., the SDP answer from one user agent doesn't include any coder included in the offer previously sent by the other user agent). For transcoding, the device can be configured to add media capabilities to user agents pertaining to a specific IP Group, and then perform transcoding in cases where the selected coder in the answer SDP is not one that appears in the original offer. The capabilities that can be added are one or more of the device's supported coders and are configured by using the parameter SBCExtensionCodersGroupID (points to a coders list) in the IP Profile table (which is assigned to the IP Group). Therefore, to allow user agents of different IP Groups to communicate with each other (regardless of their capabilities), an extended coders table with at least one coder that is supported by each IP Groups' user agents needs to be

assigned to each IP Group. Therefore, each offer destined to specific IP Groups include this coder.

In the scenario depicted in the figure below, the IP phone on the LAN side initiates a call to the IP phone on the WAN. The initial SDP offer (from the LAN leg) includes codec G.711 as its supported codec. Since this is sent to a Destination IP Group that is configured with an extended coder list, on the WAN leg the device adds another supported codec G.729 to the SDP, which is now offered to the WAN IP phone. The WAN IP phone chooses the extended codec (G.729) in its SDP answer to the device's WAN leg. Since this codec was not included in the original incoming offer, the device performs transcoding (between G.729 and G.711) between its two legs, allowing the streaming of media to occur.

**Figure 32-4: Transcoding using Extended Coders (Example)**



For an SDP offer to provide an extended coder list to a remote user agent, the following prerequisites must be fulfilled:

- An extended coders list has been configured for the user agent's IP Group (i.e., Destination IP Group)
- The incoming offer contains at least one supported coder (otherwise, transcoding can't be performed)
- Both legs have available DSP's
- T.38 doesn't appear in the offer

If the above prerequisites are not met, the SDP offer is sent without the extended coders list. The coders from the extended list are added after the ones from the original offer (decreases transcoding probability). Coders common between the extended coders list and those in the original SDP offer are not added. Transcoding may be performed even in scenarios when the same coder has been chosen - this occurs if the coders use different coder parameters (e.g. rate and packetization time).

The device also supports early media, whereby the first offer\answer transaction is finalized and the media flow starts before the SIP call is connected (before the INVITE 200 OK response). The offer and 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 ReINVITE SIP transactions. The media handling is similar to the original offer/answer handling. If the offer is rejected by the remote party, then no media changes occur (e.g. INVITE without SDP, then 200 OK and ACK, offer\answer within an offer/answer, and Hold ReINVITE with IP address of 0.0.0.0 - IP address is unchanged).

### 32.4.3 No Media Anchoring

The No Media Anchoring or Anti-Tromboning feature enables the use of SBC signaling capabilities without handling the RTP/SRTP (media) flow between remote SIP user agents (UA). The RTP packet flow does not traverse the device and instead, the two SIP UAs establish a direct RTP/SRTP flow (i.e., direct call) between one another. Signaling continues to traverse the device with minimal intermediation and involvement to enable certain SBC abilities such as routing.

By default, media packets traverse the device. This is done in order to:

- Solve NAT problems
- Enforce media security policy
- Perform media transcoding between the two legs
- Media monitoring

However, since media packets traverse the SBC, media quality may degrade, for example, due to packet delay.

In some setups, specific calls do not require media anchoring, for example, when there is no need for NAT, security, or transcoding. This is typical for calls between users in the LAN:

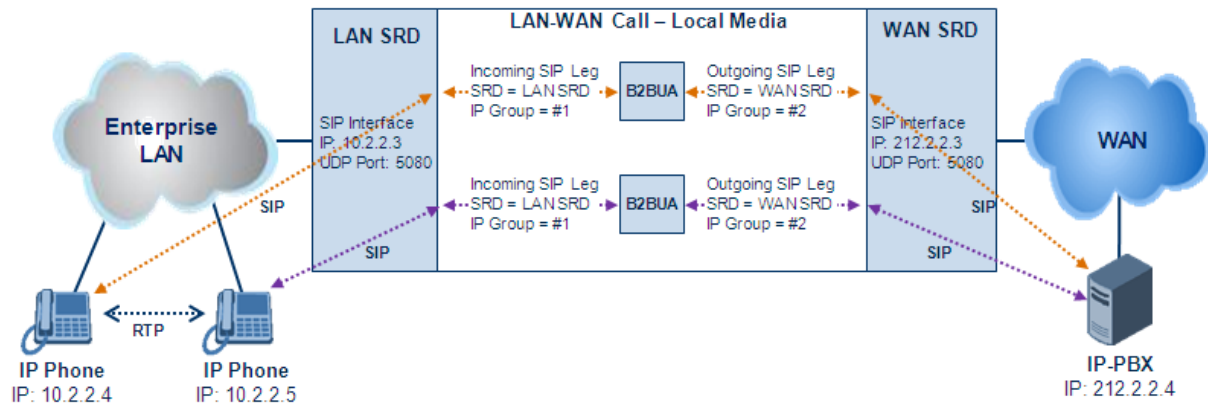
- Internal LAN calls: When the SBC routes a call between two UAs within the same LAN, the SBC can forward the SDP directly between caller and callee, and direct the RTP to flow between the UAs without traversing the SBC.
- Internal LAN calls via WAN: In this setup, the SBC dynamically identifies that the call is between UAs located in the same network (i.e., LAN) and thereby, directs the RTP to flow between these UAs without traversing the SBC

In contrast to the regular SBC implementation, the No Media Anchoring feature:

- Does not perform any manipulation on SDP data (offer/answer transaction) such as ports, IP address, coders
- Opening voice channels and allocation of IP media ports are not required

The No Media Anchoring feature is typically implemented in the following scenarios:

- SBC device is located within the LAN.
- Calls between two SIP UA's in the same LAN and signals are sent to a SIP proxy server (or hosted IP PBX) located in the WAN.

**Figure 32-5: SBC SIP Signaling without RTP Media Flow**


The benefits of implementing the No Media Anchoring include the following:

- Saves network bandwidth
- Reduces CPU usage (no RTP/SRTP handling)
- Avoids interference in SDP negotiation and header manipulation on RTP/SRTP

The No Media Anchoring process is as follows:

1. Identifies a No Media Anchoring call - according to configuration and the call's properties (such as source, destination, IP Group, and SRD).
2. Handles the identified No Media Anchoring call.

The No Media Anchoring feature is enabled using the SBCDirectMedia parameter. You can also enable No Media Anchoring per SRD (using the IntraSRDMediaAnchoring parameter), whereby calls between two UA's that pertain to the same SRD (source and destination) are handled as No Media Anchoring (direct media) calls.

#### Notes:

- No Media Anchoring can be used when the SBC does not do NAT traversal (for media) where all the users are in the same domain.
- No Media Anchoring calls cannot operate simultaneously with the following SBC features:
  - Force transcoding
  - Extension Coders
  - Extension of RFC 2833/Out-of-band DTMF/In-band DTMF
  - Extension of SRTP/RTP
All restriction features (Allowed Coders, restrict SRTP/SRT, restrict RFC 2833) can operate simultaneously. Once No Media Anchoring is enabled, the features listed above are disabled.
- The Coder Restriction feature operates simultaneously with No Media Anchoring calls. Restricted coders are removed from the SDP offer message.
- When two UA's pertain to the same SRD, the parameter IntraSRDMediaAnchoring is set to 1, and one of the UA's is defined as a foreign user (example, "follow me service") located in the WAN, while the other UA is located in the LAN: calls between these two UA's can't be established until IntraSRDMediaAnchoring is set to 0, as the device doesn't interfere in the SIP signaling. In other words, parameters such as IP addresses are not manipulated for calls between LAN and WAN (although required).
- When the parameter SBCDirectMedia is disabled, No Media Anchoring calls between two UA's belonging to separate SRD's cannot be configured. No Media Anchoring calls between two UA's belonging to the same SRD is configurable only (in this case).



### 32.4.4 Transcoding Modes

The device supports the configuration of the voice transcoding mode (media negotiation) between the two SBC legs. The device can be configured to perform transcoding only when necessary. Typically, the SBC passes RTP packets transparently (RTP-to-RTP) between the two user agents. If the device is configured to always perform transcoding, then transcoding is performed on the outgoing SBC leg and the device's SBC application interworks the media by implementing PSTN transcoding (since both legs have different media capabilities).

In the SBC application, forced transcoding of voice in an SBC session allows the device to receive capabilities that are not negotiated between the SBC legs. For example, if on the SBC session you want to force Gain Control to use voice transcoding even though both sides of the session have negotiated without SBC intervention (for example, coder extension).

The transcoding mode can be configured using the parameters `TranscodingMode` and `IPProfile`.



**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.

### 32.4.5 Restricting Coders

The SBC Allowed Coders (coders restriction) feature determines the coders that can be used for a specific SBC leg. This provides greater control over bandwidth by enforcing the use of specific coders (*allowed coders groups*) while preventing the use of other coders. This is done by defining a group of allowed coders for the SBC leg, as described below:

1. Configure a Coders Group for allowed coders, using the `AllowedCodersGroup` parameter.
2. Select this Coders Group using the `SBCAllowedCodersGroupID` parameter of the IP Profile table.
3. Enable this feature by setting the `SBCAllowedCodersMode` parameter of the IP Profile table to **Restriction**.

Coders that are not listed (including unknown coders) in the Allowed Coders Group are removed from the SDP offer. Therefore, only coders common between the SDP offer and Allowed Coders Group are used. If the SDP offer does not list any of the Allowed Coders, the call is rejected, unless transcoding is configured (using Extension coders – see 'Coder Transcoding' on page 432).



**Notes:**

- For a list of supported coders, see 'Configuring Coders' on page 233.
- Allowed Coders Groups are applicable only to audio media.

The Allowed Coders process is as follows:

- a. The device receives an incoming SIP message with SDP (offer) and checks the offered coders.
- b. The source (first) leg may have Allowed Coders (i.e. list of coders that can be used - enforced).
- c. The device checks for common coders between the SDP offered coders and the Allowed Coders Group list.

For example, assume the following:

- The SDP offer includes the following coders: G.729, G.711, and G.723.
- The source (first) leg includes the following Allowed Coders: G.711 and G.729.

The device selects the common coders, i.e., G.711 and G.729 (with changed preferred coder priority - highest for G.711). In other words, it removes the coders that are not in the Allowed Coders list and the order of priority is first according to the Allowed Coders list.

### 32.4.6 Coder Transcoding

The device can add coders, referred to as *Extension coders* to the SDP offer in the outgoing leg.

For example, assume the following:

- The SDP offer includes the following coders: G.729, G.711, and G.723.
  - The incoming leg includes the following Allowed coders: G.711 and G.729.
1. The device selects the common coders, i.e., G.711 and G.729 (with changed preferred coder priority - highest for G.711). In other words, it removes the coders that are not in the Allowed coders list and the order of priority is first according to the Allowed coders list.
  2. Assuming that the outgoing leg also includes Allowed coders and/or Extension coders: The device performs the Allowed coders procedure (common coders) between the updated coder list and the outgoing leg's Allowed coders. The Extension coders procedure is performed before Allowed coders.
  3. Adding to the example, assume the following:
    - For the outgoing leg, the device selects the common coders G.711 and G.729 (explained in the example above).
    - Outgoing leg includes the Extended coder G.726.
    - Outgoing leg includes the following Allowed coders: G.723, G.726, and G.729.

As a result, the device selects the common coders, i.e., G.729 and G.726 (coder priority did not change Extension coder order).

If the Allowed coders policy on the SDP incoming leg returns an empty coders list, the device rejects the call (SIP 488 or ACK and BYE). If both Extension coders and Allowed coders policies on SDP (in this order) returns an empty coders list, the outgoing leg rejects the call (SIP 488, or ACK and BYE).

Below is an example, assuming that Allowed Coders list (ordered) includes G711A-law (PCMA), G729, and G711U-law (PCMU), and Extension Coder is G729.

1. SDP offer - original offer:

```
m=audio 6050 RTP/AVP 0 8 4 96
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
```

2. SDP offer - after manipulation:

```
m=audio 6010 RTP/AVP 8 0 96 18
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
```

```
aptime:20
a=sendrecv
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
```

In the SDP, the "m=audio 6010 RTP/AVP 8 0 96 18" line shows that the coder priority has changed - G.711A-law ("8") and then G.711U-law ("0") - and that the Extension coder G.729 ("18") has been added. The G.723 coder ("4") in the original offer was removed as it was not defined in the Allowed Coders list (i.e., a restricted coder).

➤ **To configure Extension coders:**

1. In the Coders Group table (see 'Configuring Coder Groups' on page 236), configure a Coders Group for extension coders.
2. In the IP Profile table, select this Coders Group in the 'Extension Coders Group ID' parameter.
3. In the IP Profile table, enable this feature by setting the 'Allowed Coders Mode' parameter to **Restriction** or **Restriction and Preference**.

### 32.4.7 Prioritizing Coder List in SDP Offer

In addition to restricting the use of coders with Allowed coders, the device can prioritize the coders listed in the SDP offer. This feature is referred to as *Coder Preference*. This is done on both SBC legs:

- **Incoming SDP offer:** The device arranges the coder list according to the order in the Allowed Coders Group table. The coders listed higher up in the table take preference over ones listed lower down in the table. This feature is enabled by setting the 'Allowed Coders Mode' parameter in the IP Profile table to **Preference** or **Restriction and Preference**. If set to **Preference**, in addition to the Allowed coders that are listed first in the SDP offer, the original coders received in the SDP are retained and listed after the Allowed coders. Thus, this mode does not necessarily restrict coder use to Allowed coders, but uses (prefers) the Allowed coders whenever possible.
- **Outgoing SDP offer:** If only Allowed coders are used, the coders are arranged in the SDP offer as described above. However, if Extension coders are also used, then the coder list is arranged according to the 'SBC Preferences Mode' parameter in the IP Profile table. This parameter can be configured to add the Extension coders after the Allowed coders (i.e., at the end of the list - default) according to their order in the Coders Group table, or arrange Allowed and Extension coders according to their position in the Coders Group table.

### 32.4.8 SRTP-RTP and SRTP-SRTP Transcoding

The device supports transcoding between SRTP and RTP. The device can also enforce specific SBC legs to use SRTP and/or RTP. The device's handling of SRTP/RTP is configured using the IP Profile parameter, SBCMediaSecurityBehaviour, which provides the following options:

- SBC passes the media as is, regardless of whether it's RTP or SRTP (default).
- SBC legs negotiate only SRTP media lines (m=); RTP media lines are removed from the incoming SDP offer\answer.
- SBC legs negotiate only RTP media lines; SRTP media lines are removed from the incoming offer\answer.
- Each SDP offer\answer is extended (if not already) to two media lines for RTP and SRTP.

If after SDP offer/answer negotiation, one SBC leg uses RTP while the other uses SRTP, then the device performs RTP-SRTP transcoding. To translate between RTP and SRTP, the following prerequisites must be met:

- At least one supported SDP "crypto" attribute.
- The EnableMediaSecurity parameter must be set to 1.

Channel resources are not required for transcoding between RTP and SRTP.

Transcoding where both legs are configured for SRTP is typically required to trans-encrypt and trans-decrypt. This is relevant when the MKI and Symmetric MKI parameters are enabled. In other words, both sides need to both encrypt and decrypt the outgoing and incoming SRTP packets, respectively. Channel resources are not required for transcoding between SRTP and SRTP.

### 32.4.9 Multiple RTP Media Streams per Call Session

The device's SBC application supports multiple RTP media streams per SBC call session. Up to five different media types can be included in a session:

- Audio (m=audio)
- Video (m=video)
- Text (m=text)
- Fax (m=image)

Therefore, the device can provide transcoding of various attributes in the SDP offer/answer (e.g., codec, port, and packetization time) per media type. If the device is unable to perform transcoding (for example, does not support the codec), it relays the SBC dialog transparently.

### 32.4.10 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 this parameter to determine the DTMF method for the leg.
  - **[0]** (default): the device does not attempt to interwork any special DTMF method
  - **[1]**: In Band
  - **[2]**: INFO, Cisco
  - **[3]**: INFO, Nortel
  - **[4]**: INFO, Korea

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.

## 32.5 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 IP Profile and Coder Group Settings tables. The IP Profile table determines the supported fax coders and the negotiation method used between the incoming and outgoing fax legs, using the following fax-related parameters:

- 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.
- SBCFaxCodersGroupID: defines the supported fax coders (from the Coders Group Settings table).
- SBCFaxOfferMode: determines the fax coders sent in the outgoing SDP offer.
- SBCFaxAnswerMode: determines the fax coders sent in the outgoing SDP answer.



**Note:** The voice-related coder configuration (Allowed and Extended 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 Coders Group table, it is not used for fax processing even if it is listed in the Coders Group Settings table for faxes. However, support for G.711 coders for voice is not dependent upon which fax coders are listed in the Coders Group Settings table.

## 32.6 Limiting SBC Call Duration

You can define a maximum allowed duration (in minutes) for SBC calls. If an established call reaches this user-defined limit, the device terminates the call. This feature ensures calls are properly terminated, allowing available resources for new calls. This feature is configured using the MaxCallDuration parameter.

## 32.7 SIP Authentication Server for SBC Users

The device can function as an authentication server for SIP SBC message requests, based on HTTP authentication DIGEST with MD5. Alternatively, such requests can be authenticated by an external, third-party server.

When functioning as an authentication server (set by the IP Group table parameter, AuthenticationMode), the device authenticates users belonging to a User-type IP Group. When the device receives an INVITE or REGISTER request from a client (e.g., SIP phone) for SIP message authorization, the device processes the authorization as follows:

1. The device verifies the type of incoming SIP method (e.g., INVITE) that must be challenged for authorization. This is configured using the IP Group table parameter, MethodList.

2. If the message is received without an Authorization header, the device "challenges" the client by sending a 401 or 407 SIP response. The client then resends the request with an Authorization header (containing the user name and password).
3. The device validates the SIP message according to the settings of the parameters, AuthNonceDuration, AuthChallengeMethod and AuthQOP.
  - If validation fails, the message is rejected and the device sends a 403 "Forbidden" response.
  - If validation succeeds, the device verifies identification of the SBC user. This is done by checking that the user name and password received from the user is the same username and password that appears in the device's database. The SBC users in the database are obtained from the User Information file. If the SIP SBC user is not successfully authenticated after three attempts, the device sends a 403 "Forbidden" response.
4. If the user is successfully identified, the SIP message request is processed.

## 32.8 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.

### 32.8.1 Interworking SIP 3xx Redirect Responses

The device supports interworking of SIP 3xx redirect responses. By default, the device's handling of SIP 3xx responses is to send the Contact header unchanged. However, some SIP UAs may support different versions of the SIP 3xx standard while others may not even support SIP 3xx.

The handling of SIP 3xx can be configured for all calls, using the global parameter SBC3xxBehavior. For configuring different SIP 3xx handling options for different UAs (i.e., per IP Group), use the IP Profile table parameter, 'SBC Remote 3xx Behavior'.

#### 32.8.1.1 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.



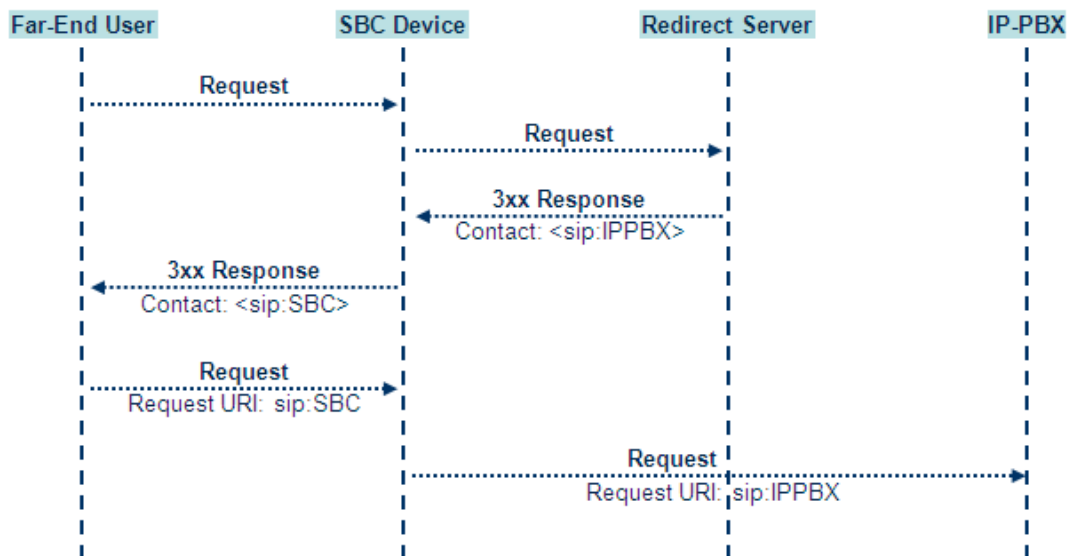
The device enforces this by modifying each Contact in the 3xx response as follows:

- 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.
5. The prefix is removed before the resultant INVITE is sent to the destination.

**Figure 32-6: SIP 3xx Response Handling**



The process of this feature is described using an example:

1. The device receives the Redirect server's SIP 3xx response (e.g., Contact: <sip:User@IPPBX:5060;transport=tcp;param=a;q=0.5).
2. 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).
3. The device sends this manipulated SIP 3xx response to the Far-End User (FEU).
4. 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).
5. 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).
6. 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).

### 32.8.1.2 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).

## 32.8.2 Interworking SIP Diversion and History-Info Headers

This device can be configured to interwork between the SIP Diversion and History-Info headers. This is important, for example, to networks that support the Diversion header but not the History-Info header, or vice versa. Therefore, mapping between these headers is crucial for preserving the information in the SIP dialog regarding how and why (e.g., call redirection) the call arrived at a certain SIP UA.

This feature is configured in the IP Profile table (IPProfile parameter) using the following new parameters:

- SBCDiversionMode - defines the device's handling of the Diversion header
- SBCHistoryInfoMode - defines the device's handling of the History-Info header

The handling of the SIP Diversion and History-Info headers is described in the table below:

**Handling of SIP Diversion and History-Info Headers**

Parameter Value	SIP Header Present in Received SIP Message		
	Diversion	History-Info	Diversion and History-Info
<b>HistoryInfoMode = Add</b> <b>DiversionMode = Remove</b>	Diversion converted to History-Info. Diversion removed.	Not present	Diversion removed.
<b>HistoryInfoMode = Remove</b> <b>DiversionMode = Add</b>	Not present.	History-Info converted to Diversion. History-Info removed.	History-Info added to Diversion. History-Info removed.
<b>HistoryInfoMode = Disable</b> <b>DiversionMode = Add</b>	Diversion converted to History-Info.	Not present.	Diversion added to History-Info.
<b>HistoryInfoMode = Disable</b> <b>DiversionMode = Add</b>	Not present.	History-Info converted to Diversion.	History-Info added to Diversion.
<b>HistoryInfoMode = Add</b> <b>DiversionMode = Add</b>	Diversion converted to History-Info.	History-Info converted to Diversion.	Headers are synced and sent.

Parameter Value	SIP Header Present in Received SIP Message		
<b>HistoryInfoMode = Remove</b> <b>DiversionMode = Remove</b>	Diversion removed.	History-Info removed.	Both removed.

### 32.8.3 Interworking SIP REFER Messages

The device supports interworking of SIP REFER messages. SIP UAs may support different versions of the REFER standard while others may not even support REFER.

This feature supports the following:

- Attended, unattended, and semi-attended call transfers
- Sending INVITE, REFER-notifications, BYE, PRACK and Session Timer on behalf of peer PBXs
- Advanced routing rules for the new, initiated INVITE
- Forwarding early media after REFER while attempting to avoid transcoding (by sending session update)
- Interoperate with environments where different SIP UAs lack basic SIP functionality such as re-INVITE, UPDATE, PRACK, Delayed Offer, re-INVITE without SDP
- Session updates after connect to avoid transcoding

The handling of REFER can be configured for all calls, using the global parameter `SBCReferBehavior`. For configuring different REFER handling options for different UAs (i.e., IP Groups), use the IP Profile table parameter, 'SBC Remote Refer Behavior'.

- **Local handling of REFER:** This option is used for UAs that do not support REFER. Upon receipt of a REFER request, instead of forwarding it to the IP Group, the device handles it locally. It generates a new INVITE to the alternative destination according to the rules in the IP-to-IP Routing table (where the 'Call Trigger' field is set to **REFER**). It is also possible to specify the IP Group that sent the REFER request, as matching criteria for the re-routing rule in this table ('ReRoute IP Group ID' field).
- **Transparent handling:** The device forwards the REFER with the Refer-To header unchanged.
- **Re-routing through SBC:** The device changes the Refer-To header so that the re-routed INVITE is sent through the SBC application.
- **IP Group Name =** The device sets the host part in the REFER message to the name configured for the IP Group in the IP Group table.

### 32.8.4 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.

## 32.8.5 Interworking SIP Session Timer

The device supports interworking of the SIP signaling keep-alive mechanism. The SIP standard provides a signaling keep-alive mechanism using re-INVITE and UPDATE messages. In certain setups, keep-alive may be required by some SIP UAs while for others it may not be supported. The device can resolve this mismatch by performing the keep-alive process on behalf of SIP UAs that do not support it.

For configuring the handling of session expires, use the IP Profile parameter, 'SBC Session Expires Mode'.

## 32.8.6 Interworking SIP Early Media

The device supports various interworking modes for SIP early media between SIP UAs (i.e., IP Groups):

- **Early Media Enabling:** The device supports the interworking of early media between SIP UAs that support early media and those that do not support receipt of early media. Early media can arrive in provisional responses to an INVITE request. The device forwards the request of early media for IP Groups that support this capability; otherwise, the device terminates it. Provisional responses whose SDP are suppressed are changed to a SIP 180 response. This feature is also supported for delayed offers. This is configured using the IP Profile parameter, 'SBC Remote Early Media Support'. The device refers to this parameter also for features that require early media such as playing ringback tone.
- **Early Media Response Type:** The device supports the interworking of different SIP provisional response types between UAs for forwarding the early media to the caller. This can support all early media response types (default), SIP 180 only, or SIP 183 only, and is configured by the IP Profile parameter, 'SBC Remote Early Media Response Type'.
- **Multiple 18x:** The device supports the interworking of different support for multiple 18x responses (including 180 Ringing, 181 Call is Being Forwarded, 182 Call Queued, and 183 Session Progress) that are forwarded to the caller. The UA can be configured as supporting only receipt of the first 18x response (i.e., the device forwards only this response to the caller), or receipt of multiple 18x responses (default). This is configured by the IP Profile parameter, 'SBC Remote Multiple 18x Support'.
- **Early Media RTP:** The device supports the interworking with remote clients that send 18x responses with early media and whose subsequent RTP is delayed, and with remote clients that do not support this and require RTP to immediately follow the 18x response. Some clients do not support 18x with early media, while others require 18x with early media (i.e., they cannot play ringback tone locally). These various interworking capabilities are configured by the IP Profile parameters, 'SBC Remote Early Media RTP', 'SBC Remote Supports RFC 3960', and 'SBC Remote Can Play Ringback'. See the flowcharts below for the device's handling of such scenarios:

Figure 32-7: SBC Early Media RTP 18x without SDP

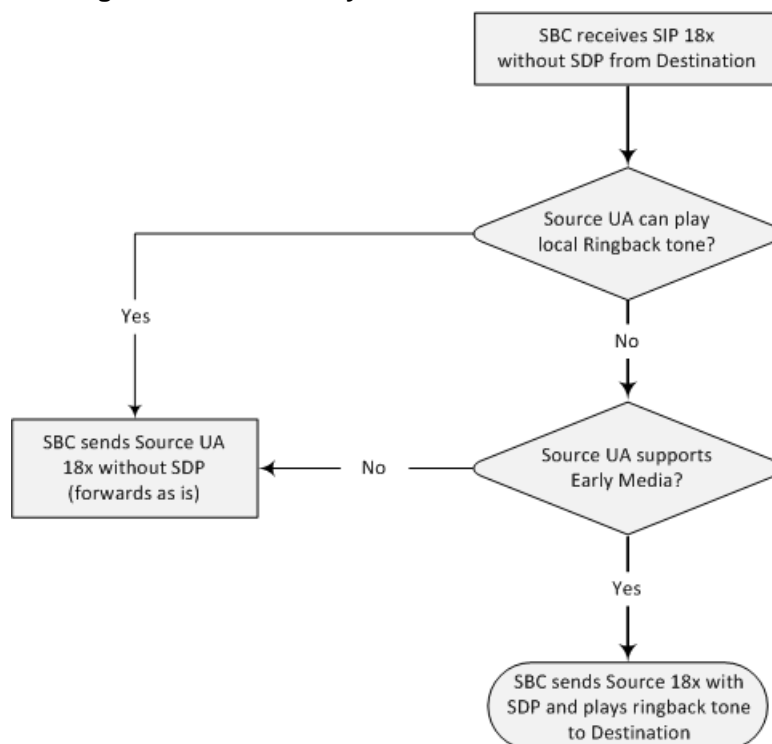
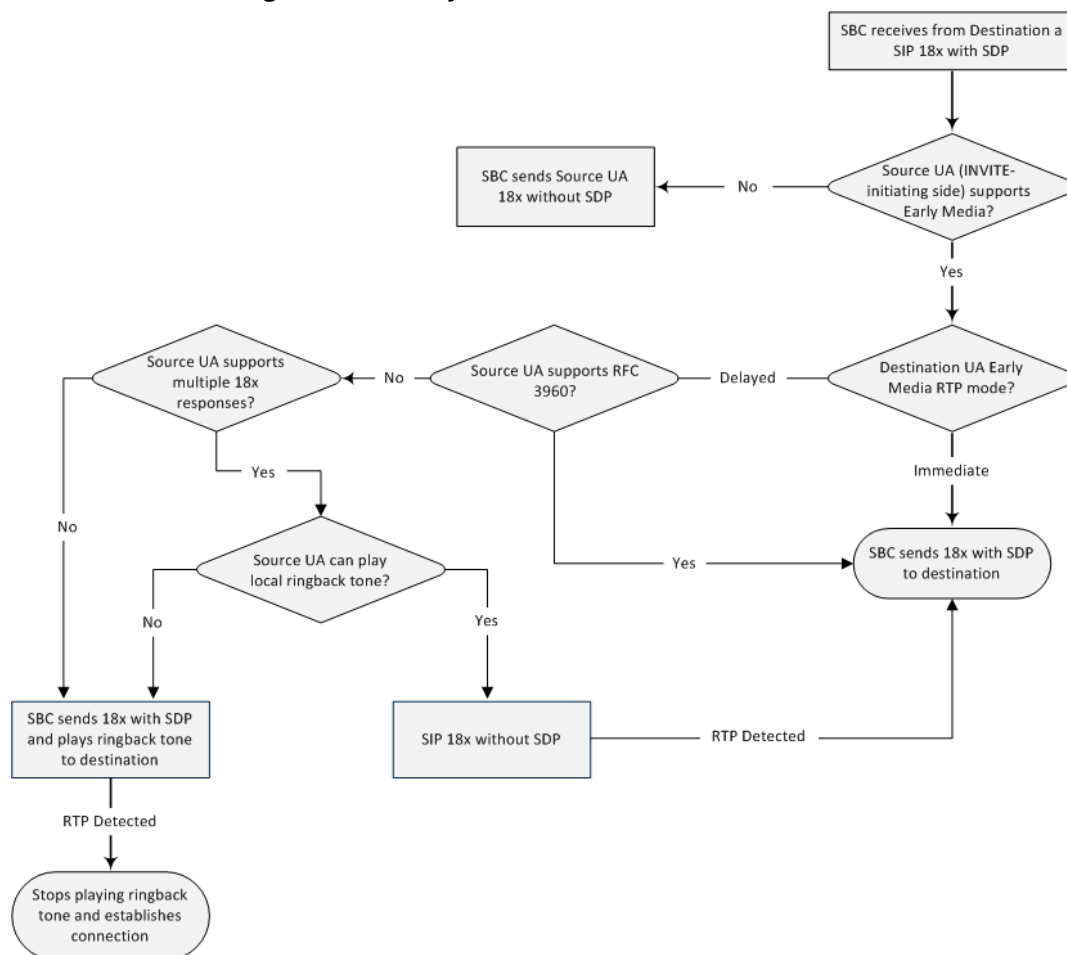


Figure 32-8: Early Media RTP - SIP 18x with SDP



### 32.8.7 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'.

### 32.8.8 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'.

### 32.8.9 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.

### 32.8.10 Interworking Delayed Offer

The device enables sessions between endpoints (IP Groups) that send INVITES without SDP (i.e., delayed media) and those that do not support the receipt of INVITES without SDP. The device creates an SDP and adds it to INVITES that arrive without SDP. This intervention in the SDP offer/answer process may require transcoding. Delayed offer is also supported when early media is present.

The interworking of delayed offer is configured using the IP Profile parameter 'SBC Remote Delayed Offer Support'.



**Note:** For this feature to function properly, a valid Extension Coders Group ID needs to be configured for IP Profiles that do not support delayed offer.

### 32.8.11 Interworking Call Hold

The device supports the interworking of call hold / retrieve requests between IP entities supporting different call hold capabilities:

- Interworking SDP call hold formats. This is configured by the IP Profile parameter, 'SBC Remote Hold Format'.
- Interworking the play of the held tone for IP entities that cannot play held tones locally. This is configured by the IP Profile parameter, 'SBC Play Held Tone'.
- Interworking generation of held tone where the device generates the tone to the held party instead of the call hold initiator. This is configured by the IP Profile parameter, 'SBC Reliable Held Tone Source'.

For configuring IP Profiles, see Configuring IP Profiles [239](#).

## 32.9 Call Survivability

This section describes various call survivability features supported by the SBC device.

### 32.9.1 Auto-Provisioning of Subscriber-Specific Information for BroadWorks Server for Survivability

This feature enables SBC user registration for interoperability with BroadSoft BroadWorks server to provide call survivability in case of connectivity failure with the BroadWorks server, for example, due to a WAN failure. This feature enables local users to dial a local extension (or any other configured alias) that identifies another local user, in survivability mode. This feature is enabled using the SBCExtensionsProvisioningMode parameter.

In normal operation, when subscribers (such as IP phones) register to the BroadWorks server through the device, the device includes the SIP Allow-Events header in the sent REGISTER message. In response, the BroadWorks server sends the device a SIP 200 OK containing an XML body with subscriber information such as extension number, phone number, and URIs (aliases). The device forwards the 200 OK to the subscriber (without the XML body).

**Figure 32-9: Interoperability with BroadWorks Registration Process**



The device saves the users in its registration database with their phone numbers and extensions, enabling future routing to these destinations during survivability mode. When in survivability mode, the device routes the call to the Contact associated with the dialed phone number or extension number in the registration database.

Below is an example of an XML body received from the BroadWorks server:

```
<?xml version="1.0" encoding="utf-8"?>
<BroadsoftDocument version="1.0" content="subscriberData">
  <phoneNumbers>
    <phoneNumber>2403645317</phoneNumber>
    <phoneNumber>4482541321</phoneNumber>
  </phoneNumbers>
  <aliases>
    <alias>sip:bob@broadsoft.com</alias>
  </aliases>
</BroadsoftDocument>
```



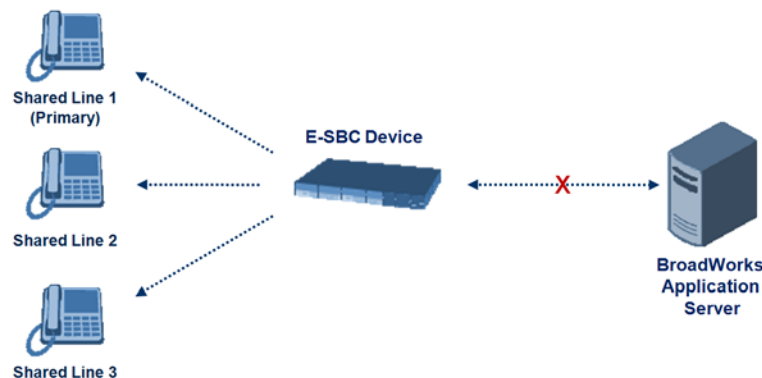
```
<alias>sip:rhughes@broadsoft.com</alias>
</aliases>
<extensions>
  <extension>5317</extension>
  <extension>1321</extension>
</extensions>
</BroadSoftDocument>
```

### 32.9.2 BroadSoft's Shared Phone Line Call Appearance for SBC Survivability

The device can provide redundancy for BroadSoft's Shared Call Appearance feature. When the BroadSoft application server switch (AS) fails or does not respond, or when the network connection between the device and the BroadSoft AS is down, the device manages the Shared Call Appearance feature for the SIP clients.

This feature is supported by configuring a primary extension and associating it with secondary extensions (i.e., *shared lines*) so that incoming calls to the primary extension also ring at the secondary extensions. The call is established with the first extension to answer the call, and consequently, the ringing at the other extensions stop. For example, assume primary extension number 600 is shared with secondary extensions 601 and 602. In the case of an incoming call to 600, all three phone extensions ring simultaneously (using the device's call forking feature as described in 'SIP Forking Initiated by SIP Proxy Server' on page 448). Note that incoming calls specific to extensions 601 or 602 ring only at these specific extensions.

**Figure 32-10: Call Survivability for BroadSoft's Shared Line Appearance**



To configure this capability, you need to configure a shared-line, inbound manipulation rule for registration requests to change the destination number of the secondary extension numbers (e.g. 601 and 602) to the primary extension (e.g., 600). Call forking must also be enabled. The procedure below describes the main configuration required.



**Notes:**

- You can configure whether REGISTER messages from secondary lines are terminated on the device or forwarded transparently (as is), using the SBCSharedLineRegMode parameter.
- The device enables outgoing calls from all equipment that share the same line simultaneously (usually only one simultaneous call is allowed per a specific shared line).
- The LED indicator of a shared line may display the wrong current state.



➤ **To configure the Shared Line feature:**

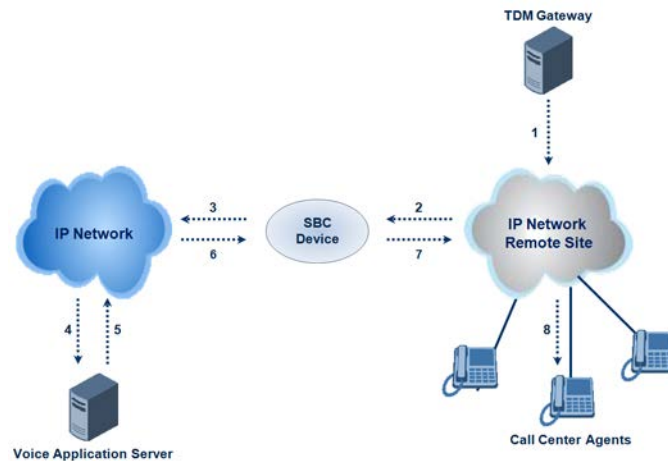
1. In the IP Group table (see 'Configuring IP Groups' on page 204), add a Server-type IP Group for the BroadWorks server.
2. In the IP Group table, add a User-type IP Group for the IP phone users and set the 'Enable SBC Client Forking' parameter to **Yes** so that the device forks incoming calls to all contacts under the same AOR that are registered in the device's registration database.
3. In the IP-to-IP Routing table (see 'Configuring SBC IP-to-IP Routing' on page 462), add a rule for routing calls between the above configured IP Groups.
4. In the IP to IP Inbound Manipulation table (see 'Configuring IP-to-IP Inbound Manipulations' on page 471), add a manipulation rule for the secondary extensions (e.g., 601 and 602) so that they also register in the device's database under the primary extension contact (e.g., 600):
  - Set the 'Manipulation Purpose' field to **Shared Line**.
  - Set the 'Source IP Group' field to the IP Group ID that you created for the users (e.g., 2).
  - Set the 'Source Username Prefix' field to represent the secondary extensions (e.g., 601 and 602).
  - Set the 'Manipulated URI' field to **Source** to manipulate the source URI.
  - Set the 'Remove From Right' field to "1" to remove the last digit of the extensions (e.g., 601 is changed to 60).
  - Set the 'Suffix to Add' field to "0" to add 0 to the end of the manipulated number (e.g., 60 is changed to 600).

### 32.9.3 Call Survivability for Call Centers

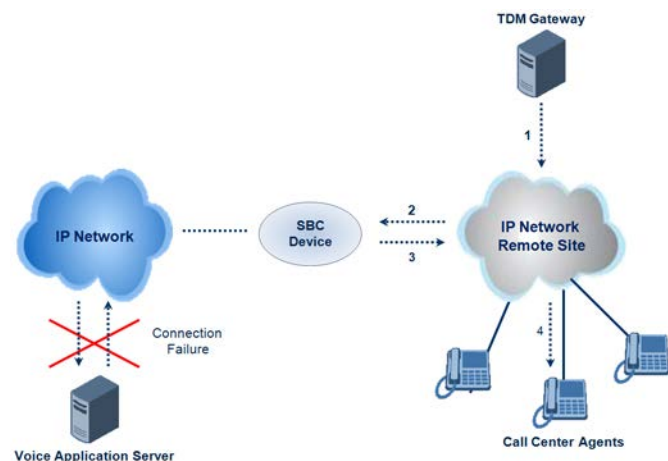
The device supports call survivability for call centers. When a communication failure (e.g., in the network) occurs with the remote voice application server responsible for handling the call center application (such as IVR), the device routes the incoming calls received from the customer (i.e., from the TDM gateway) to the call center agents.

In normal operation, the device registers the agents in its users registration database. Calls received from the TDM gateway are forwarded by the device to the application server, which processes the calls and sends them to specific call center agents, through the device. Upon a failure with the application server, the device routes the calls from the TDM Gateway to the agents. The device routes the call to the first available user it finds. If the call is not answered by the user, the device routes it to the next available user. The SBC can handle a sequence of up to five users, after which the session is timed out and the call is dropped.

**Figure 32-11: Normal Operation in Call Center Application**



**Figure 32-12: Call Survivability for Call Center**



➤ **To configure call survivability for a call center application:**

1. In the IP Group table (see 'Configuring IP Groups' on page 204), 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 456), add rules to classify incoming calls that are received from the entities listed in Step 1, to IP Groups.
3. In the SBC IP-to-IP Routing table (see 'Configuring SBC IP-to-IP Routing' on page 462), add the following IP-to-IP routing rules:
  - For normal operation:
    - ◆ Routing from TDM Gateway to Application server.
    - ◆ Routing from Application server to call center agents.
  - For call survivability mode: Routing from TDM Gateway to call center agents. This configuration is unique due to the following settings:
    - ◆ The 'Source IP Group ID' field is set to the IP Group of the TDM Gateway.

- ◆ The 'Destination Type' field is set to **Hunt Group**, which is specifically used for call center survivability.
- ◆ The 'Destination IP Group ID' field is set to the IP Group of the call center agents.

The figure below displays a routing rule example, assuming IP Group "1" represents the TDM Gateway and IP Group "3" represents the call center agents:

**Figure 32-13: Routing Rule Example for Call Center Survivability**

<b>Add Record</b> <span>✕</span>	
Index	3
Source IPGroup ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All ▼
Message Condition	None ▼
Destination Type	Hunt Group ▼
Destination IPGroup ID	3
Destination SRD ID	None ▼
Destination Address	
Destination Port	0
Destination Transport Type	▼
Alternative Route Options	Route Row ▼
Cost Group	None ▼
<input type="button" value="Submit"/> <input type="button" value="✕ Cancel"/>	

### 32.9.4 Survivability Mode Display on Aastra IP Phones

If the SBC device is deployed in an Enterprise network with Aastra IP phones and connectivity with the WAN fails, the device provides call survivability by enabling communication between IP phone users within the LAN enterprise. In such a scenario, the device can be configured to notify the IP phones that it is currently operating in Survivability mode. When this occurs, the Aastra IP phones display the message, "StandAlone Mode" on their LCD screens. This feature is enabled by setting the `SBCEnableAASTRASurvivabilityNotice` parameter to 1.

When this feature is enabled and the SBC device is in Survivability mode, it responds to SIP REGISTER messages from the IP phones with a SIP 200 OK containing the following XML body:

```
Content-Type: application/xml
<?xml version="1.0" encoding="utf-8"?>
<LMIDocument version="1.0">
  <LocalModeStatus>
    <LocalModeActive>true</LocalModeActive>
    <LocalModeDisplay>StandAlone Mode</LocalModeDisplay>
  </LocalModeStatus>
</LMIDocument>
```

```
</LocalModeStatus>  
</LMIDocument>
```

## 32.10 Call Forking

This section describes various Call Forking features supported by the device.

### 32.10.1 Initiating SIP Call Forking

The SBC device supports call forking of an incoming call to multiple SBC users (destinations). Call forking is supported by the device's capability of registering multiple SIP client user phone contacts (mobile and fixed-line extensions) under the same Address of Record (AOR) in its registration database. This feature can be implemented in the following example scenarios:

- An enterprise Help Desk, where incoming customer calls are simultaneously sent to multiple customer service agent extensions.
- An employee's phone devices, where the incoming call is simultaneously sent to multiple devices (e.g., to the employee's office phone and mobile SIP phone).
- An enterprise reception desk, where an incoming call is simultaneously sent to multiple receptionists.

The device supports various modes of call forking. For example, in Parallel call forking mode, the device sends the INVITE message simultaneously to all the users registered under the same AOR, resulting in the ringing of all extensions; the first extension to pick up the call receives the call, and all other extensions stop ringing. The Call Forking feature is configured by creating a User-type IP Group and configuring the IP Group table's parameter, 'SBC Client Forking Mode' (see [Configuring IP Groups](#) on page 204).

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.

### 32.10.2 SIP Forking Initiated by SIP Proxy Server

The device can handle SIP forking responses received from a proxy server in response to an INVITE forwarded by the device from a UA. In other words, received responses with a different SIP To header 'tag' parameter for the request forwarded by the device. This occurs in scenarios, for example, where a proxy server forks the INVITE request to several UAs, and therefore, the SBC device may receive several replies for a single request. Forked SIP responses may result in a single SDP offer with two or more SDP answers during call setup. The SBC handles this scenario by "hiding" the forked responses from the INVITE-initiating UA. This is achieved by marking the UA that responded first to the INVITE as the active UA, and only requests/responses from that UA are subsequently forwarded. All other requests/responses from other UAs are handled by the SBC (SDP offers from these users are answered with an 'inactive' media).

The SBC supports two forking modes, configured by the `SBCForkingHandlingMode` parameter:

- Latch On First - only the first received 18x response is forwarded to the INVITE initiating UA, and disregards any subsequently received 18x forking responses (with or without SDP).
- Sequential - all 18x responses are forwarded to the INVITE initiating UA, one at a time in a sequential manner. If 18x arrives with an offer only, only the first offer is forwarded to the INVITE initiating UA.

The SBC also supports media synchronization for call forking. If the active UA is the first one to send the final response (e.g., 200 OK), the call is established and all other final responses are acknowledged and a BYE is sent if needed. If another UA sends the first

final response, then it is possible that the SDP answer that was forwarded to the INVITE-initiating UA is not relevant, and media synchronization is needed between the two UAs. Media synchronization is done by sending a re-INVITE request immediately after the call is established. The re-INVITE is sent without an offer to the INVITE-initiating UA. This causes the UA to send an offer which is forwarded to the UA that confirmed the call. The media synchronization process is enabled by the EnableSBCMediaSync parameter.

## 32.11 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.

## Reader's Notes

## 33 SBC Configuration

This section describes the configuration of the SBC application.



**Note:** For the SBC application, the following requirements must be met:

- The SBC application must be enabled (see 'Enabling Applications' on page 197).
- The 'SBC' Software License Key must be installed on the device (see 'Software License Key' on page 552).

### 33.1 Configuring General Settings

The General Settings page allows you to configure general SBC parameters. For a description of these parameters, see 'SBC Parameters' on page 873.

➤ **To configure general parameters:**

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

**Figure 33-1: General Settings Page**

Transcoding Mode	Only If Required
SBC No Answer Timeout	600
SBC GRUU Mode	AsProxy
Minimum Session-Expires [sec]	90
BroadWorks Survivability Feature	Disable
Bye Authentication	Disable
SBC User Registration Time	0
SBC Proxy Registration Time	0
SBC Survivability Registration Time	0
SBC Forking Handling Mode	Latch On First
Allow Unclassified Calls	Reject
SBC Session-Expires [sec]	180
SBC Direct Media	Disable
<b>Server Authentication</b>	
Lifetime of the nonce in seconds	300
Authentication Challenge Method	0
Authentication Quality of Protection	2

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 33.2 Configuring Admission Control

The Admission Control page allows you to define up to 100 rules for limiting the number of concurrent calls (SIP dialogs). These call limits can be applied per SRD, IP Group, SIP request type (e.g., INVITEs), SIP dialog direction (e.g., inbound), and/or per user (identified by its registered contact). This is especially important for applications where VoIP and Data traffic contend on the WAN throughput, which may be limited by itself. For example, DSL WAN access interface is very limited in the uplink. Therefore, by controlling the number of calls allowed, bandwidth can be reserved for specific Data applications. This feature can be useful for implementing Service Level Agreements (SLA) policies.

The SIP dialog limits can be defined per SIP request type and direction. These relate to requests that initiate SIP dialogs and not the subsequent requests that can be of different type and direction. The SIP dialog-initiating request types can include SIP INVITEs, REGISTER, and/or SUBSCRIBE, or it can be configured to include the total number of all dialogs.

This feature also provides support for SIP-dialog rate control, using the "token bucket" mechanism. The token bucket is a control mechanism that dictates the rate of SIP-dialog setups based on the presence of tokens in the bucket – a logical container that holds aggregate SIP dialogs to be accepted or transmitted. Tokens in the bucket are removed ("cached in") for the ability to setup a dialog. Therefore, a flow can setup dialogs up to its peak burst rate if there are adequate tokens in the bucket and if the burst threshold is configured appropriately:

- Every SIP dialog setup request must attempt to take a token from the bucket.
- If there are no tokens, the request is dropped.
- New tokens are added to the bucket at a user-defined rate (token rate).
- If the bucket contains the maximum number of tokens, tokens to be added at that moment are dropped.

Requests that reach the user-defined call limit (maximum concurrent calls and/or call rate) are sent to an alternative route, if configured in the IP-to-IP Routing table for the SRD or IP Group. If no alternative routing rule is located, the device rejects the SIP request with a SIP 486 "Busy Here" response.



### Notes:

- The enforcement of a configured limitation for the incoming leg is performed immediately after the Classification process. If the call/request is rejected at this stage, no routing is performed. The enforcement for the outgoing leg is performed within each alternative route iteration. This is accessed from two places: one during initial classification/routing, and another during alternative routing process.
- The Admission Control table can also be configured using the table *ini* file parameter, `SBCAdmissionControl` or CLI command, `configure voip > sbc sbc-admission-control`.



➤ **To configure Admission Control rules:**

1. Open the Admission Control page (**Configuration** tab > **VoIP** menu > **SBC** > **Admission Control**).
2. Click the **Add** button; the following dialog box appears:

**Figure 33-2: Admission Control Page - Add Record Dialog Box**

Add Record	
Index	0
Limit Type	IP Group
IP Group ID	-1
SRD ID	-1
Request Type	All
Request Direction	Both
Limit	-1
Limit Per User	-1
Rate	0
Max Burst	0
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Configure the rule as required. For a description of the parameters, see the table below.
4. Click **Submit** to apply your changes.

**Admission Control Parameters**

Parameter	Description
Limit Type CLI: limit-type [SBCAdmissionControl_LimitType]	Defines the entity to which the rule applies. <ul style="list-style-type: none"> <li>▪ [0] IP Group (default)</li> <li>▪ [1] SRD</li> </ul>
IP Group ID CLI: ip-group-id [SBCAdmissionControl_IPGroupID]	Defines the IP Group to which you want to apply the rule. To apply the rule to all IP Groups, set this parameter to -1 (default). <b>Note:</b> This parameter is applicable only if 'Limit Type' is set to <b>IP Group</b> .
SRD ID CLI: srd-id [SBCAdmissionControl_SRDID]	Defines the SRD to which you want to apply the rule. To apply the rule to all SRDs, set this parameter to -1 (default). <b>Note:</b> This parameter is applicable only if 'Limit Type' is set to <b>SRD</b> .
Request Type CLI: request-type [SBCAdmissionControl_RequestType]	Defines the SIP dialog-initiating request type to which you want to apply the rule (not the subsequent requests that can be of different type and direction). <ul style="list-style-type: none"> <li>▪ [0] All = (Default) Includes the total number of all dialogs.</li> <li>▪ [1] INVITE</li> <li>▪ [2] SUBSCRIBE</li> <li>▪ [3] Other</li> </ul>

Parameter	Description
Request Direction CLI: request-direction <b>[SBCAdmissionControl_RequestDirection]</b>	Defines the direction of the SIP request to which the rule applies. <ul style="list-style-type: none"> <li><b>[0]</b> Both = (Default) Rule applies to inbound and outbound SIP dialogs.</li> <li><b>[1]</b> Inbound = Rule applies only to inbound SIP dialogs.</li> <li><b>[2]</b> Outbound = Rule applies only to outbound SIP dialogs.</li> </ul>
Limit CLI: limit <b>[SBCAdmissionControl_Limit]</b>	Defines the maximum number of concurrent SIP dialogs per IP Group or SRD. You can also use the following special values: <ul style="list-style-type: none"> <li><b>[0]</b> 0 = Block all these dialogs.</li> <li><b>[-1]</b> -1 = (Default) No limit.</li> </ul>
Limit Per User CLI: limit-per-user <b>[SBCAdmissionControl_LimitPerUser]</b>	Defines the maximum number of concurrent SIP dialogs per user belonging to the specified IP Group or SRD. You can also use the following special values: <ul style="list-style-type: none"> <li><b>[0]</b> 0 = Block all these dialogs.</li> <li><b>[-1]</b> -1 = (Default) No limit.</li> </ul>
Rate CLI: rate <b>[SBCAdmissionControl_Rate]</b>	Defines the rate at which tokens are added to the token bucket per second (i.e., token rate). One token is added to the bucket every 1000 divided by the value of this parameter (in milliseconds). The default is 0 (i.e., unlimited rate). <b>Note:</b> The token bucket feature is per IP Group, SRD, SIP request type, and SIP request direction.
Max Burst CLI: max-burst <b>[SBCAdmissionControl_MaxBurst]</b>	Defines the maximum number of tokens (SIP dialogs) that the bucket can hold. The device only accepts a SIP dialog if a token exists in the bucket. Once the SIP dialog is accepted, a token is removed from the bucket. If a SIP dialog is received by the device and the token bucket is empty, then the device rejects the SIP dialog. Alternatively, if the bucket is full, for example, 100 tokens, and 101 SIP dialogs arrive (before another token is added to the bucket, i.e., faster than that defined in the Rate field), then the device accepts the first 100 SIP dialogs and rejects the last one.  Dropped requests are replied with the SIP 486 "Busy Here" response. Dropped requests are not counted in the bucket.  The default is 0 (i.e., unlimited SIP dialogs). <b>Note:</b> The token bucket feature is per IP Group, SRD, SIP request type, and SIP request direction.

## 33.3 Configuring Allowed Coder Groups

The Allowed Coders Group page allows you to define up to five Allowed Coder Groups, each with up to 10 coders. Allowed Coder Groups determine the coders that can be used for a specific SBC leg. Therefore, the device can enforce the use of specific coders while preventing the use of other coders. Coders excluded from the Allowed Coders Group are removed from the SDP offer. Only common coders between SDP offered coders and coders configured in the Allowed Coder Groups are used. For more information, see 'Restricting Coders' on page 431.

The Allowed Coders Group table is also used to configure Extension coders. These are coders that are added to the SDP offer. For more information on Extension coders, see Coder Transcoding on page 432.

The order of appearance of coders in the Allowed Coder Group determines the coder priority (preference), whereby the first coder is given the highest priority. For more information, see 'Prioritizing Coder List in SDP Offer' on page 433.

**Notes:**

- Each coder can appear only once per Allowed Coder Group.
- Allowed Coder Groups are applicable only to audio media.
- Allowed Coder Groups can be assigned to IP Profiles (see 'Configuring IP Profiles' on page 239).
- The Allowed Coder Groups table can also be configured using the table ini file parameter, AllowedCodersGroup or CLI command, configure voip > sbc allowed-coders-group group0.

➤ **To configure Allowed Coder Groups:**

1. Open the Allowed Coders Group page (**Configuration** tab > **VoIP** menu > **SBC** > **Allowed Coders Group**).

**Figure 33-3: Allowed Coders Group Page**

2. From the 'Allowed Coders Group ID' drop-down list, select an ID for the Allowed Coder Group.
3. In the Coder Name table, select coders for the Allowed Coder Group.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 532.

## 33.4 Routing SBC

This section describes the configuration of the routing entities for the SBC application. These include the following:

- Classification rules - see 'Configuring the Classification Rules' on page 456
- Condition rules - see 'Configuring Condition Rules' on page 461
- IP-to-IP routing rules - see 'Configuring SBC IP-to-IP Routing' on page 462
- Alternative routing reasons - see 'Configuring Alternative Routing Reasons' on page 468

### 33.4.1 Configuring Classification Rules

The Classification table enables you to configure up to 100 Classification rules. Classification rules are used to classify incoming SIP dialog-initiating requests (e.g., INVITE messages) to source IP Groups from where the SIP dialog request originated. The identified IP Group is later used in the manipulation and routing processes.

Classification rules also enhance security by allowing you to create a SIP access list, whereby classified calls can be denied (i.e., blacklist) or allowed (i.e., whitelist).

The Classification table is used to classify incoming SIP dialog requests only if the other classification stages fail, as described below:

1. **Classification Stage 1 - Registered Users Database:** The device searches its registration database to check if the incoming SIP dialog arrived from a registered user:
  - Compares the SIP Contact header of the received SIP dialog to the Contact of the registered user.
  - Compares the URL in the SIP P-Asserted-Identity/From header to the registered address-of-record (AOR).

If this stage fails, the device proceeds to classification based on Proxy Set.

2. **Classification Stage 2 - Proxy Set:** If the database search fails, the device performs classification based on Proxy Set if the 'Classify By Proxy Set' parameter is enabled for the IP Group (see 'Configuring IP Groups' on page 204). If enabled, the device checks whether the INVITE's IP address (if host names, then according to the dynamically resolved IP address list) is defined for a Proxy Set ID (in the Proxy Set table). If a Proxy Set ID has such an IP address, the device classifies the INVITE to the IP Group that is associated with this Proxy Set. (The Proxy Set ID is assigned to the IP Group using the IP Group table's 'Proxy Set ID' parameter.)



**Note:** For security purposes, it is highly recommended to disable the Classify by Proxy Set feature so that the device can use the Classification table instead, for "strict" classification of incoming calls to IP Groups. In addition, in cases where multiple IP Groups are associated with the same Proxy Set ID, do **not** use the Classify by Proxy Set feature.

If this stage fails (or Classify by Proxy Set is disabled), the device proceeds to classification based on the Classification table.

3. **Classification Stage 3 - Classification Table:** If classification based on Proxy Set fails (or disabled), the device uses the Classification table to classify the SIP dialog to an IP Group. If it locates a classification rule whose characteristics (such as source IP address) match the incoming SIP dialog, then the SIP dialog is assigned to the associated IP Group. In addition, if the classification rule is defined as a whitelist, the SIP dialog is allowed and proceeds with the manipulation, routing and other SBC processes. If the classification rule is defined as a blacklist, the SIP dialog is denied.

If the classification process fails, the device rejects or allows the call, depending on the setting of the 'Unclassified Calls' parameter (on the General Settings page - **Configuration** tab > **VoIP** menu > **SBC** > **General Settings**). If this parameter is set to **Allow**, the incoming SIP dialog is assigned to an IP Group as follows:

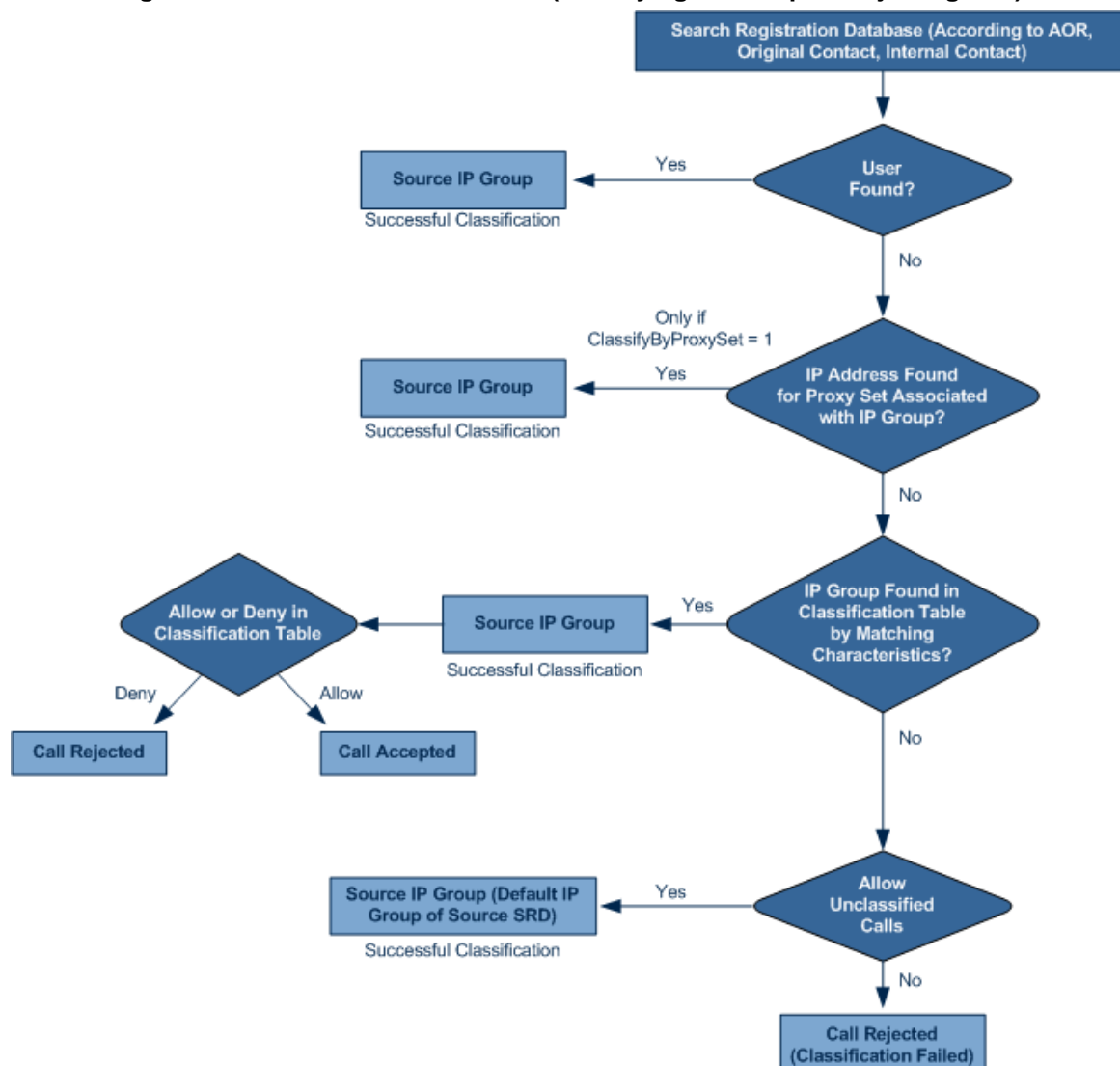
1. The device checks on which SIP listening port (e.g., 5061) the incoming SIP dialog request arrived and the SIP Interface which is configured with this port (in the SIP Interface table).
2. The device checks the SRD that is associated with this SIP Interface (in the SIP Interface table) and then classifies the SIP dialog with the first IP Group that is associated with this SRD. For example, if IP Groups 3 and 4 use the same SRD, the device classifies the call to IP Group 3.



**Note:** If classification for a SIP request fails and the device is configured to reject unclassified calls, the device can send a specific SIP response code per SIP interface, configured by the 'Classification Failure Response Type' parameter in the SIP Interface table (see 'Configuring SIP Interface Table' on page 201).

The flowchart below illustrates the classification process:

**Figure 33-4: Classification Process (Identifying IP Group or Rejecting Call)**



**Notes:**

- Incoming REGISTER messages are saved in the device's registration database and sent to a destination only if they are associated with a source User-type IP Group.
- The Classification table can also be configured using the table ini file parameter, Classification or CLI command, configure voip > sbc routing classification.

The Classification table provides two configuration areas:

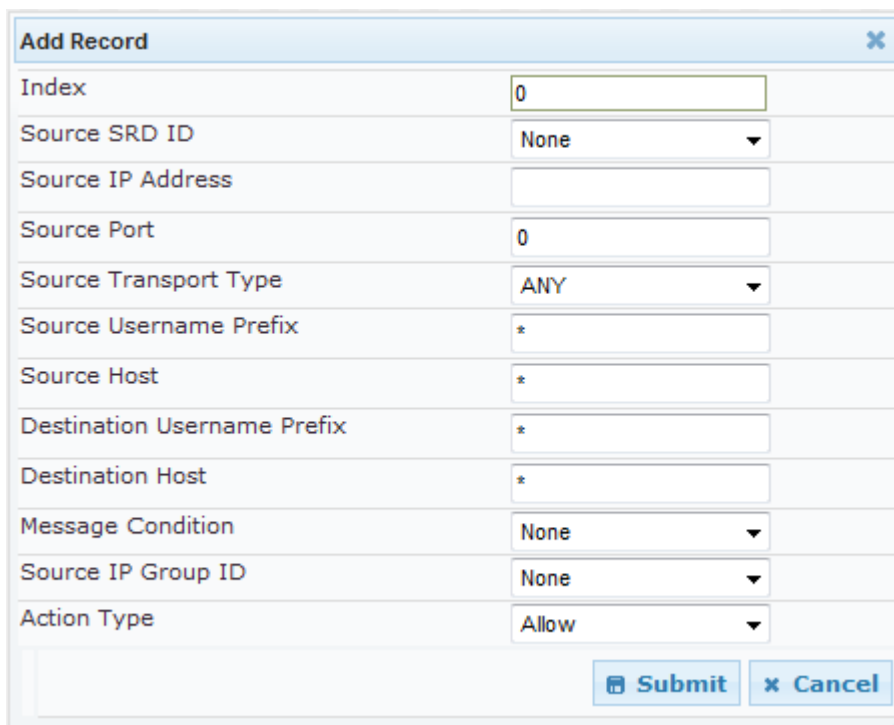
- Matching characteristics of incoming IP call, for example, source IP address.
- Operation - classifies call to an IP Group.

If the incoming call matches the characteristics of a rule, then the call is classified to the IP Group configured for that rule.

➤ **To configure classification rules:**

1. Open the Classification Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Classification Table**).
2. Click the **Add** button; the following appears:

**Figure 33-5: Classification Table Page**



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

3. Configure the rule as required. For a description of the parameters, see the table below.
4. Click **Submit** to apply your changes.

**Classification Table Parameters**

Parameter	Description
Index	Defines the index number of the table row entry.
<b>Matching Characteristics</b>	
Source SRD ID CLI: src-srd-id [Classification_SrcSRD ID]	<p>Defines the SRD ID of the incoming SIP dialog. The default is -1 (i.e., no SRD is assigned).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>■ The SRDs are configured in the SRD table (see 'Configuring SRD Table' on page 199).</li> <li>■ The SRDs are also associated with a port number as defined by the SIP Interface used by the SRD (see 'Configuring SIP Interface Table' on page 201).</li> </ul>
Source IP Address	Defines the source IP address (in dotted-decimal notation) of the

Parameter	Description
CLI: src-ip-address <b>[Classification_SrcAddress]</b>	incoming SIP dialog. <b>Notes:</b> <ul style="list-style-type: none"> <li>If this parameter is not configured or is configured as an asterisk (*), then any source IP address is accepted.</li> <li>The IP address can include the "x" wildcard to represent single digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99.</li> <li>The IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255.</li> </ul>
Source Port CLI: src-port <b>[Classification_SrcPort]</b>	Defines the source port number of the incoming SIP dialog.
Source Transport Type CLI: src-transport-type <b>[Classification_SrcTransportType]</b>	Defines the source transport type (UDP, TCP, or TLS) of the incoming SIP dialog.
Source Username Prefix CLI: src-user-name-prefix <b>[Classification_SrcUsernamePrefix]</b>	Defines the prefix of the source URI user part of the incoming SIP dialog. The URI is typically located in the SIP From header. However, you can configure the SIP header from where the device obtains the source URI. This is done in the IP Group table, using the 'Source URI Input' parameter. For more information on how the device obtains this URI, see 'SIP Dialog Initiation Process' on page 420. <b>Notes:</b> <ul style="list-style-type: none"> <li>For REGISTER requests, the source URL is obtained from the To header.</li> <li>The prefix can be a single digit or a range of digits. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659.</li> </ul>
Source Host CLI: src-host <b>[Classification_SrcHost]</b>	Defines the prefix of the source URI host name. The URI is typically located in the SIP From header. However, you can configure the SIP header from where the device obtains the source URI. This is done in the IP Group table, using the 'Source URI Input' parameter. For more information on how the device obtains this URI, see 'SIP Dialog Initiation Process' on page 420. If this routing rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any source host prefix. <b>Note:</b> For REGISTER requests, the source URL is obtained from the To header.
Destination Username Prefix CLI: dst-user-name-prefix <b>[Classification_DestUsernamePrefix]</b>	Defines the prefix of the destination Request-URI user part of the incoming SIP dialog. <b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659.
Destination Host CLI: dst-host <b>[Classification_DestHost]</b>	Defines the prefix of the destination Request-URI host name of the incoming SIP dialog request. If this routing rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any destination host prefix.



Parameter	Description
Message Condition CLI: message-condition <b>[Classification_MessageCondition]</b>	Assigns a Condition rule which can also be used to classify the incoming SIP dialog. <b>Note:</b> Condition rules are configured in the Condition Table (see 'Configuring Condition Rules' on page 461).
<b>Operation Rule</b>	
Source IP Group ID CLI: src-ip-group-id <b>[Classification_SrcIPGroupID]</b>	Defines an IP Group to which the incoming SIP dialog request is assigned if this SIP dialog matches the matching rule. The default is -1 (i.e., no IP Group is assigned). <b>Notes:</b> <ul style="list-style-type: none"> <li>The IP Group must be associated with the selected SRD.</li> <li>The IP Group is used for SBC routing and manipulations.</li> <li>To define IP Groups, see 'Configuring IP Groups' on page 204.</li> </ul>
Action Type CLI: action-type <b>[Classification_ActionType]</b>	Defines a whitelist or blacklist for incoming SIP dialog requests that match the characteristics of the classification rule. <ul style="list-style-type: none"> <li><b>[0]</b> Deny = Blocks incoming SIP dialogs that match the characteristics of the Classification rule (blacklist).</li> <li><b>[1]</b> Allow = Allows incoming SIP dialogs that match the characteristics of the Classification rule (whitelist) and assigns it to the associated IP Group. (default)</li> </ul>

### 33.4.1.1 Classification Based on URI of Selected Header Example

The following example describes how to configure classification of incoming calls to IP Groups, based on source URI in a specific SIP header.

This example assumes the following incoming INVITE message:

```
INVITE sip:8000@10.33.4.226 SIP/2.0
Via: SIP/2.0/UDP 10.33.4.226;branch=z9hG4bKVEBTDAHSUYRTEXEDEGJY
From: <sip:100@10.33.4.226>;tag=YSQQKXXREVDPTYPTNFMWG
To: <sip:8000@10.33.4.226>
Call-ID: FKPNOYRNKROIMEGBSSKS@10.33.4.226
CSeq: 1 INVITE
Contact: <sip:100@10.33.4.226>
Route: <sip:2000@10.10.10.10>,<sip:300@10.10.10.30>
Supported: em,100rel,timer,replaces
P-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 ID
0	333	-	-	1
1	1111	2000	10.10.10.10	2



2. In the IP Group table, add the following IP Groups:

Index	Source URI Input	Destination URI Input
1	-	-
2	P-Called-Party-ID	Route

In this example, a match exists only for Classification Rule #1. This is because the source (1111) and destination (2000) username prefixes match those in the INVITE's P-Called-Party-ID header (i.e., "<sip:1111@10.33.38.1>") and Route header (i.e., "<sip:2000@10.10.10.10>"), respectively. These SIP headers were determined in IP Group ID 2.

### 33.4.2 Configuring Condition Rules

Condition rules define special conditions for the incoming SIP messages. Condition rules are configured using the same syntax as that used for message conditions in the Message Manipulations table (see Configuring SIP Message Manipulation on page 226).

Condition rules are used if assigned to any of the following:

- Classification rules in the Classification table (see Configuring Classification Rules on page 456). This enables you to use SIP message conditions as an additional matching criteria for classifying incoming SIP dialogs to IP Groups, thereby increasing the strictness of the classification process.
- IP-to-IP routing rules in the IP-to-IP Routing table (see Configuring SBC IP-to-IP Routing on page 462): This enables you to use SIP message conditions as an additional matching criteria for selecting the routing rule.

You can define simple Condition rules, for example, "header.to.host contains company" or complex rules using the "AND" or "OR" Boolean operands. You can also use regular expressions (regex), for example:

- "body.sdp regex pcmu" can be used to enable routing based on the offered codec (G.711 Mu) in the incoming SDP message.
- "body.sdp regex (AVP[0-9][\s]\*\s8[\s][\n])" can be used to enable routing based on payload type 8 in the incoming SDP message.

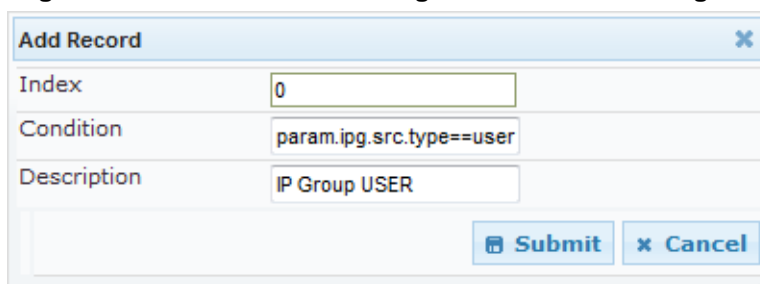


#### Notes:

- For a description on SIP message manipulation syntax, For a detailed description of the syntax for configuring SIP message manipulation rules, refer to *SIP Message Manipulations Quick Reference Guide*.
- The Condition table can also be configured using the table ini file parameter, ConditionTable or CLI command, configure voip > sbc routing condition-table.

#### ➤ To configure Condition rules:

1. Open the Condition Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Condition Table**).
2. Click the **Add** button; the following dialog box appears:

**Figure 33-6: Condition Table Page - Add Record Dialog Box**


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

The figure below shows an example of the Condition table configured with the following rules:

- **Index 1:** Incoming SIP dialog that is classified as belonging to a User-type IP Group.
- **Index 2:** Incoming SIP dialog with a SIP Via header.
- **Index 3:** Incoming SIP dialog with 101 as the user part in the SIP From header.

**Figure 33-7: Condition Table Page**

Index	Condition	Description
0	param.ipg.src.type==user	IP Group USER
1	header.via.exists	Includes SIP Via header
2	header.from.url.user=='101'	101 user part of From header

**Condition Table Parameters Description**

Parameter	Description
Condition CLI: condition [ConditionTable_Condition]	Defines the Condition rule of the SIP message. The valid value is a string. <b>Note:</b> User and host parts must be enclosed in single quotes.
Description CLI: description [ConditionTable_Description]	Defines a brief description of the Condition rule.

### 33.4.3 Configuring SBC IP-to-IP Routing

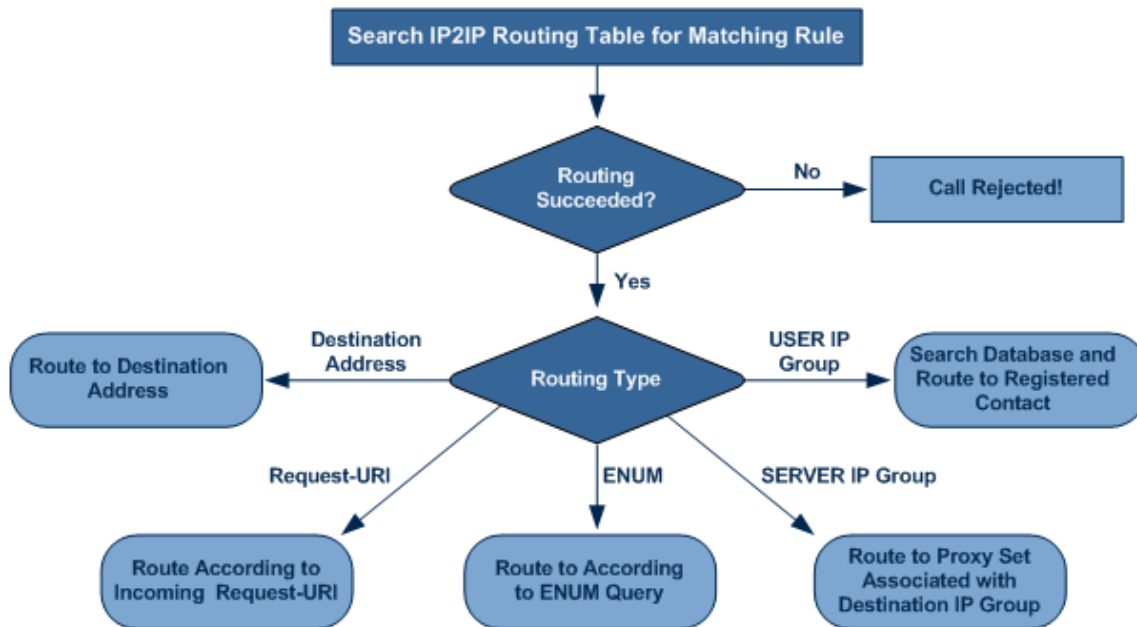
The IP-to-IP Routing table enables you to configure up to 200 SBC IP-to-IP routing rules. This table provides enhanced IP-to-IP call routing capabilities for routing received SIP dialog messages (e.g., INVITE) to a destination IP address. The SIP message is routed according to a routing rule whose configured input characteristics (e.g., Source IP Group) match the incoming SIP message. If the characteristics of an incoming call does not match the first rule, the call characteristics is then compared to those of the second rule, and so on until a matching rule is located. If no rule is matched, the call is rejected.

The call can be routed to one of the following IP destinations:

- Registered user Contact listed in the device's database (only for User-type IP Groups).
- IP Group - the destination is the address configured for the Proxy Set associated with the IP Group (allows redundancy/load balancing).
- Specified destination address (can be based on IP address, host name, port, transport type, and/or SRD). Routing to a host name can be resolved using NAPTR/SRV/A-Record.

- Request-URI of incoming SIP dialog initiating requests.
- ENUM query.
- Hunt Group - used for call survivability (see 'Call Survivability for Call Centers' on page 445).
- IP address (in dotted-decimal notation or FQDN - NAPTR/SRV/A-Record resolutions) according to a specified Dial Plan index listed in the loaded Dial Plan file.
- LDAP server or LDAP query result. For more information on LDAP-based routing, see 'Routing Based on LDAP Active Directory Queries' on page 179.

Figure 33-8: IP-to-IP Routing Types



For all destination types listed above except destination IP Group, the IP Group can optionally be itself, configured to provide the destination SRD and/or IP Profile. If neither destination SRD nor destination IP Group is defined, the destination SRD is the source SRD and the destination IP Group is its default IP Group.

The IP-to-IP Routing table also provides the following features:

- **Alternative routing or load balancing:** In addition to the alternative routing/load balancing provided by the Proxy Set associated with the destination IP Group, the table allows the configuration of alternative routes whereby if a route fails, the next adjacent (below) rule in the table that is configured as 'Alt Route Ignore/Consider Inputs' are used. The alternative routes rules can be set to enforce the input matching criteria or to ignore any matching criteria. Alternative routing occurs upon one of the following conditions:
  - A request sent by the device is responded with one of the following:
    - ◆ SIP response code (i.e., 4xx, 5xx, and 6xx SIP responses) configured in the SBC Alternative Routing Reasons table (see 'Configuring Alternative Routing Reasons' on page 468).
    - ◆ SIP 408 Timeout or no response (after timeout).
  - The DNS resolution includes IP addresses that the device has yet to try (for the current call).

Messages are re-routed with the same SIP Call-ID and CSeq header fields (increased by 1).

- **Re-routing of SIP requests:** This table enables you to configure "re-routing" rules of requests (e.g., INVITEs) that the device sends upon receipt of SIP 3xx responses or REFER messages. These rules are configured for destinations that do not support

receipt of 3xx or REFER and where the device handles the requests locally (instead of forwarding the 3xx or REFER to the destination).

- **Least cost routing (LCR):** If the LCR feature is enabled, the device searches the routing table for matching routing rules and then selects the one with the lowest call cost. The call cost of the routing rule is done by assigning it a Cost Group. For configuring Cost Groups, see 'Least Cost Routing' on page 189. If two routing rules have identical costs, then the rule appearing higher up in the table (i.e., first-matched rule) is used. If a selected route is unavailable, the device uses the next least-cost routing rule. However, even if a matched rule is not assigned a Cost Group, the device can select it as the preferred route over other matched routing rules with Cost Groups, according to the settings of the LCR parameter, LCRDefaultCost (see 'Enabling LCR and Configuring Default LCR' on page 191).



**Note:** The IP-to-IP Routing table can also be configured using the table ini file parameter, IP2IPRouting (see 'SBC Parameters' on page 873) or CLI command, configure voip > sbc routing ip2ip-routing.

➤ **To configure SBC IP-to-IP routing rules:**

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Routing SBC** submenu > **IP to IP Routing Table**).
2. Click the **Add** button; the following dialog box appears:

**Figure 33-9: IP-to-IP Routing Table - Add Record Dialog Box**

Add Record	
Index	0
Source IP Group ID	-1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Destination Type	IP Group
Destination IP Group ID	-1
Destination SRD ID	None
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Cost Group	None
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

## IP-to-IP Routing Table Parameters Description

Parameter	Description
<b>Matching Characteristics</b>	
Source IP Group ID <b>[IP2IPRouting_SrcIPGroupID]</b> CLI: src-ip-group-id	Selects the IP Group from where the IP-to-IP call originated. Typically, the IP Group of an incoming SIP dialog is determined (or classified) using the 'Classification' table (see Configuring Classification Rules on page 456). If not used (i.e., any IP Group), simply leave the field empty. The default is -1.
Source Username Prefix <b>[IP2IPRouting_SrcUsernamePrefix]</b> CLI: src-user-name-prefix	Defines the prefix of the user part of the incoming SIP dialog's source URI (usually the From URI). You can use special notations for denoting the prefix. For example, to denote any prefix, use the asterisk (*) symbol; to denote calls without a user part in the URI, use the \$ sign. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659. The default is * (i.e., any prefix).
Source Host <b>[IP2IPRouting_SrcHost]</b> CLI: src-host	Defines the host part of the incoming SIP dialog's source URI (usually the From URI). If this rule is not required, leave the field empty. To denote any host name, use the asterisk (*) symbol (default).
Destination Username Prefix <b>[IP2IPRouting_DestUsernamePrefix]</b> CLI: dst-user-name-prefix	Defines the prefix of the incoming SIP dialog's destination URI (usually the Request URI) user part. You can use special notations for denoting the prefix. For example, to denote any prefix, use the asterisk (*) symbol; to denote calls without a user part in the URI, use the \$ sign. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659. The default is * (i.e., any prefix).
Destination Host <b>[IP2IPRouting_DestHost]</b> CLI: dst-host	Defines the host part of the incoming SIP dialog's destination URI (usually the Request-URI). If this rule is not required, leave the field empty. The asterisk (*) symbol (default) can be used to denote any destination host.
Request Type <b>[IP2IPRouting_RequestType]</b> CLI: request-type	Defines the SIP dialog request type of the incoming SIP dialog. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> All (default)</li> <li>▪ <b>[1]</b> INVITE</li> <li>▪ <b>[2]</b> REGISTER</li> <li>▪ <b>[3]</b> SUBSCRIBE</li> <li>▪ <b>[4]</b> INVITE and REGISTER</li> <li>▪ <b>[5]</b> INVITE and SUBSCRIBE</li> <li>▪ <b>[6]</b> OPTIONS</li> </ul>
Message Condition <b>[IP2IPRouting_MessageCondition]</b> CLI: message-condition	Selects a Message Condition rule. To configure Message Condition rules, see 'Configuring Condition Rules' on page 461.
ReRoute IP Group ID <b>[IP2IPRouting_ReRouteIPGroupID]</b> CLI: re-route-ip-group-id	Defines the IP Group that initiated (sent) the SIP redirect response (e.g., 3xx) or REFER message. This field is typically used for re-routing requests (e.g., INVITEs) when interworking is required for SIP 3xx redirect responses or REFER messages (for more information, see 'Interworking SIP 3xx Redirect Responses' on page 436 and 'Interworking SIP REFER Messages' on page 439, respectively). This parameter functions together with the 'Call Trigger' field (see below).

Parameter	Description
	The default is -1 (i.e., not configured).
Call Trigger [IP2IPRouting_Trigger] CLI: trigger	<p>Defines the reason (i.e, trigger) for re-routing the SIP request:</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Any = (Default) This routing rule is used for all scenarios (re-routes and non-re-routes).</li> <li>▪ <b>[1]</b> 3xx = Re-routes the request if it was triggered as a result of a SIP 3xx response.</li> <li>▪ <b>[2]</b> REFER = Re-routes the INVITE if it was triggered as a result of a REFER request.</li> <li>▪ <b>[3]</b> 3xx or REFER = Applies to options <b>[1]</b> and <b>[2]</b>.</li> <li>▪ <b>[4]</b> Initial only = This routing rule is used for regular requests that the device forwards to the destination. This rule is not used for re-routing of requests triggered by the receipt of REFER or 3xx.</li> </ul>
<b>Operation Routing Rule</b>	
Destination Type [IP2IPRouting_DestType] CLI: dst-type	<p>Determines the destination type to which the outgoing SIP dialog is sent.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> IP Group = (Default) The SIP dialog is sent to the IP Group's Proxy Set (SERVER-type IP Group) or registered contact from the database (if USER-type IP Group).</li> <li>▪ <b>[1]</b> Dest Address = The SIP dialog is sent to the address configured in the following fields: 'Destination SRD ID', 'Destination Address', 'Destination Port', and 'Destination Transport Type'.</li> <li>▪ <b>[2]</b> Request URI = The SIP dialog is sent to the address indicated in the incoming Request-URI. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these fields take precedence.</li> <li>▪ <b>[3]</b> ENUM = An ENUM query is sent to include the destination address. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these fields take precedence.</li> <li>▪ <b>[4]</b> Hunt Group = Used for call center survivability. For more information, see 'Call Survivability for Call Centers' on page 445.</li> <li>▪ <b>[5]</b> Dial Plan = The IP destination is determined by a Dial Plan index of the loaded Dial Plan file. The syntax of the Dial Plan index in the Dial Plan file is as follows: &lt;destination / called prefix number&gt;,0,&lt;IP destination&gt;</li> </ul> <p>Note that the second parameter "0" is ignored. An example of a configured Dial Plan (# 6) in the Dial Plan file is shown below:</p> <pre>[ PLAN6 ] 200,0,10.33.8.52      ; called prefix 200 is routed to destination 10.33.8.52 201,0,10.33.8.52 300,0,itsp.com       ; called prefix 300 is routed to destination itsp.com</pre> <p>Once the Dial Plan is defined, you need to assign it (0 to 7) to the routing rule as the destination in the 'Destination Address' parameter, where "0" denotes <b>[PLAN1]</b>, "1" denotes <b>[PLAN2]</b>, and so on.</p> <ul style="list-style-type: none"> <li>▪ <b>[7]</b> LDAP = LDAP-based routing.</li> </ul>
Destination IP Group ID [IP2IPRouting_DestIPGroupID] CLI: dst-ip-group-id	<p>Defines the IP Group ID to where you want to route the call. The SIP dialog messages are sent to the IP address defined for the Proxy Set associated with this IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Destination Address' field). However, if both parameters are configured, then the IP Group takes precedence.</p>

Parameter	Description
	<p>If the destination IP Group is of USER type, the device searches for a match between the Request-URI (of the received SIP dialog) to an AOR registration record in the device's database. The SIP dialog is then sent to the IP address of the registered contact.</p> <p>The default is -1.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is only relevant if the parameter 'Destination Type' is set to 'IP Group'. However, regardless of the settings of the parameter 'Destination Type', the IP Group is still used - only for determining the IP Profile or outgoing SRD. If neither IP Group nor SRD are defined in this table, the destination SRD is determined according to the source SRD associated with the Source IP Group (configured in the IP Group table, see 'Configuring IP Groups' on page 204). If this table does not define an IP Group but only an SRD, then the first IP Group associated with this SRD (in the IP Group table) is used.</li> <li>If the selected destination IP Group ID is type SERVER, the request is routed according to the IP Group addresses.</li> <li>If the selected destination IP Group ID is type USER, the request is routed according to the IP Group specific database (i.e., only to registered users of the selected database).</li> <li>If the selected destination IP Group ID is ANY USER ([ -2]), the request is routed according to the general database (i.e., any matching registered user).</li> </ul>
Destination SRD ID <b>[IP2IPRouting_DestSRDID]</b> CLI: dst-srd-id	<p>Defines the SRD ID. The default is None.</p> <p><b>Note:</b> The destination IP Group must belong to the destination SRD if both are configured in this table.</p>
Destination Address <b>[IP2IPRouting_DestAddress]</b> CLI: dst-address	<p>Defines the destination to where the call is sent. This can be an IP address or a domain name (e.g., domain.com).</p> <p>If ENUM-based routing is used (i.e., the 'Destination Type' parameter is set to <b>ENUM</b>) this parameter defines the IP address or domain name (FQDN) of the ENUM service, for example, e164.arpa, e164.customer.net, or NRENum.net. The device sends the ENUM query containing the destination phone number to an external DNS server, configured in the Multiple Interface table. The ENUM reply includes a SIP URI (user@host) which is used as the destination Request-URI in this routing table.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only if the 'Destination Type' parameter is set to Dest Address [1] or ENUM [3].</li> <li>When using domain names, enter a DNS server IP address or alternatively, define these names in the Internal DNS table (see Configuring the Internal SRV Table on page 121).</li> <li>To terminate SIP OPTIONS messages at the device (i.e., to handle them locally), set this parameter to "internal".</li> </ul>
Destination Port <b>[IP2IPRouting_DestPort]</b> CLI: dst-port	<p>Defines the destination port to where the call is sent.</p>
Destination Transport Type <b>[IP2IPRouting_DestTransport]</b>	<p>Defines the transport layer type for sending the call:</p> <ul style="list-style-type: none"> <li><b>[ -1 ]</b> Not Configured (default)</li> </ul>



Parameter	Description
<b>nsportType]</b> CLI: dst-transport-type	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> UDP</li> <li>▪ <b>[1]</b> TCP</li> <li>▪ <b>[2]</b> TLS</li> </ul> <p><b>Note:</b> When this parameter is set to -1, the transport type is determined by the parameter SIPTransportType.</p>
Alternative Route Options <b>[IP2IPRouting_AltRoute Options]</b> CLI: alt-route-options	<p>Determines whether this routing rule is the main routing rule or an alternative routing rule (to the rule defined directly above it in the table).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Route Row (default) = Main routing rule - the device first attempts to route the call to this route if the incoming SIP dialog's input characteristics matches this rule.</li> <li>▪ <b>[1]</b> Alt Route Ignore Inputs = If the call cannot be routed to the main route (Route Row), the call is routed to this alternative route regardless of the incoming SIP dialog's input characteristics.</li> <li>▪ <b>[2]</b> Alt Route Consider Inputs = If the call cannot be routed to the main route (Route Row), the call is routed to this alternative route only if the incoming SIP dialog matches this routing rule's input characteristics.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The alternative routing entry (<b>[1]</b> or <b>[2]</b>) must be defined in the next consecutive table entry index to the Route Row entry (i.e., directly below it). For example, if Index 4 is configured as a Route Row, Index 5 must be configured as the alternative route.</li> <li>▪ For IP-to-IP alternative routing, configure alternative routing reasons upon receipt of 4xx, 5xx, and 6xx SIP responses (see <a href="#">Configuring Alternative Routing Reasons</a> on page 468). However, if no response, ICMP, or a SIP 408 response is received, the device attempts to use the alternative route even if no entries are configured in the 'SBC Alternative Routing Reasons' table.</li> <li>▪ Multiple alternative route entries can be configured (e.g., Index 1 is the main route - Route Row - and indices 2 through 4 are configured as alternative routes).</li> </ul>
Cost Group <b>[IP2IPRouting_CostGroup]</b> CLI: cost-group	<p>Assigns a Cost Group to the routing rule for determining the cost of the call. To configure Cost Groups, see 'Configuring Cost Groups' on page 193.</p> <p>By default, no Cost Group is assigned to the rule.</p>

### 33.4.4 Configuring Alternative Routing Reasons

The SBC Alternative Routing Reasons page allows you to define up to five different call release (termination) reasons for call releases. If a call is released as a result of one of these reasons provided in SIP 4xx, 5xx, and 6xx response codes, the device attempts to locate an alternative route for the call. The call release reason type can be configured, for example, when there is no response to an INVITE message (after INVITE re-transmissions), where the device issues an internal 408 'No Response' implicit release reason.

Release reasons can also be configured to indicate that a route for an SRD or IP Group has reached its call admission control limit (i.e., maximum concurrent calls and/or call rate), as set in the Admission Control table (see 'Configuring Admission Control' on page 452). In such a scenario, an alternative route configured in the IP-to-IP Routing table can be used.

Alternative routing rules are configured in the IP-to-IP Routing table where the 'Alternative Route Options' parameter is set to **Alt Route Ignore Inputs** or **Alt Route Consider Inputs**. For more information, see 'Configuring SBC IP-to-IP Routing' on page 462.



**Notes:**

- Alternative routing occurs even if this table is not configured upon scenarios where no response, ICMP, or a SIP 408 response is received.
- SIP requests pertaining to an SRD or IP Group that reach the call limit (maximum concurrent calls and/or call rate) as defined in the Call Admission table are sent to an alternative route if configured in the IP-to-IP Routing table for the SRD or IP Group. If no alternative routing rule is located, the device automatically rejects the SIP request with a SIP 486 "Busy Here" response.
- The SBC Alternative Routing Reasons table can also be configured using the table ini file parameter, SBCAlternativeRoutingReasons or CLI command, configure voip > sbc routing sbc-alt-routing-reasons.

➤ **To configure SIP reason codes for alternative IP routing:**

1. Open the SBC Alternative Routing Reasons page (**Configuration** tab > **VoIP** menu > **SBC > Routing SBC > Alternative Routing Reasons**).

**Figure 33-10: Alternative Routing Reasons Page**

SBC Alternative Routing Reasons		
Reason 1	401	▼
Reason 2		▼
Reason 3		▼
Reason 4		▼
Reason 5		▼

2. Configure different call failure reasons that invoke alternative routing.
3. Click **Submit** to apply your changes.

## 33.5 SBC Manipulations

This section describes the configuration of the manipulation rules for the SBC application.

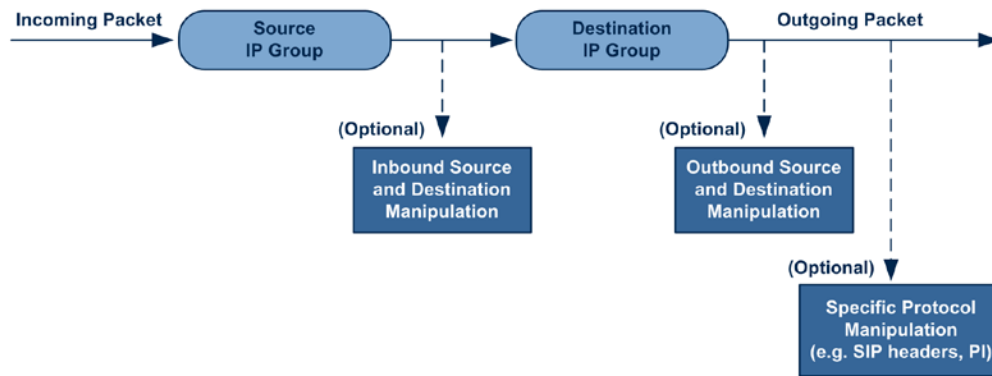


**Note:** For additional manipulation features, see the following:

- 'Configuring SIP Message Policy Rules'.
- 'Configuring SIP Message Manipulation' on page 226.

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 33-11: SIP URI Manipulation in IP-to-IP Routing**



You can also restrict source user identity in outgoing SIP dialogs in the Outbound Manipulation table (using the column PrivacyRestrictionMode). The device identifies an incoming user as restricted if one of the following exists:

- From header user is 'anonymous'.
- P-Asserted-Identity and Privacy headers contain the value 'id'.

All restriction logic is done after the user number has been manipulated.

Host name (source and destination) manipulations are simply host name substitutions with the names defined for the source and destination IP Groups respectively (if any, in the IP Group table).

Below is an example of a call flow and consequent SIP URI manipulations:

■ **Incoming INVITE from LAN:**

```

INVITE sip:1000@10.2.2.3;user=phone;x=y;z=a SIP/2.0
Via: SIP/2.0/UDP 10.2.2.6;branch=z9hGLLLLLan
From: <sip:7000@10.2.2.6;user=phone;x=y;z=a>;tag=0lLAN;parameter1=abe
To: <sip:1000@10.2.2.3;user=phone>
Call-ID: USELLLLAN@10.2.2.3
CSeq: 1 INVITE
Contact: <sip:7000@10.2.2.3>
Supported: em,100rel,timer,replaces
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK
User-Agent: Sip Message Generator V1.0.0.5
Content-Type: application/sdp
Content-Length: 155

v=0
o=SMG 791285 795617 IN IP4 10.2.2.6
s=Phone-Call
c=IN IP4 10.2.2.6
t=0 0
m=audio 6000 RTP/AVP 8
a=rtpmap:8 pcma/8000
a=sendrecv
a=ptime:20
  
```

■ **Outgoing INVITE to WAN:**

```

INVITE sip: 9721000@ITSP;user=phone;x=y;z=a SIP/2.0
Via: SIP/2.0/UDP 212.179.1.12;branch=z9hGWwan
From:
<sip:97000@IP_PBX;user=phone;x=y;z=a>;tag=OWan;parameter1=abe
To: <sip: 9721000@ ITSP;user=phone>
Call-ID: USEVWWAN@212.179.1.12
CSeq: 38 INVITE
  
```

```

Contact: <sip:7000@212.179.1.12>
Supported: em,100rel,timer,replaces
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER
User-Agent: Sip Message Generator V1.0.0.5
Content-Type: application/sdp
Content-Length: 155
v=0
o=SMG 5 9 IN IP4 212.179.1.11
s=Phone-Call
c=IN IP4 212.179.1.11
t=0 0
m=audio 8000 RTP/AVP 8
a=rtpmap:8 pcma/8000
a=sendrecv
a=ptime:20

```

The SIP message manipulations in the example above (contributing to typical topology hiding) are as follows:

- Inbound source SIP URI user name from "7000" to "97000":

```

From:<sip:7000@10.2.2.6;user=phone;x=y;z=a;tag=01LAN;parameter1=abe

```

to

```

From:
<sip:97000@IP_PBX;user=phone;x=y;z=a;tag=0Wan;parameter1=abe

```

- Source IP Group name (i.e., SIP URI host name) from "10.2.2.6" to "IP\_PBX":

```

From:<sip:7000@10.2.2.6;user=phone;x=y;z=a;tag=01LAN;parameter1=abe

```

to

```

From:
<sip:97000@IP_PBX;user=phone;x=y;z=a;tag=0Wan;parameter1=abe

```

- Inbound destination SIP URI user name from "1000" to "9721000":

```

INVITE sip:1000@10.2.2.3;user=phone;x=y;z=a SIP/2.0
To: <sip:1000@10.2.2.3;user=phone>

```

to

```

INVITE sip:9721000@ITSP;user=phone;x=y;z=a SIP/2.0
To: <sip:9721000@ITSP;user=phone>

```

- Destination IP Group name (SIP URI host name) from "10.2.2.3" to "ITSP":

```

INVITE sip:1000@10.2.2.3;user=phone;x=y;z=a SIP/2.0
To: <sip:1000@10.2.2.3;user=phone>

```

to

```

INVITE sip:9721000@ITSP;user=phone;x=y;z=a SIP/2.0
To: <sip:9721000@ITSP;user=phone>

```

### 33.5.1 Configuring IP-to-IP Inbound Manipulations

The IP to IP Inbound Manipulation table allows you to configure up to 100 manipulation rules for manipulating the source or destination SIP URI user part of inbound SIP dialog requests. You can apply these manipulations to different SIP dialog message types (e.g., INVITE or REGISTER) and SIP headers as follows:

- Manipulated destination URI user part are done on the following SIP headers: Request-URI, To, and Remote-Party-ID (if exists)

- Manipulated source URI user part are done on the following SIP headers: From, P-Asserted-Identity (if exists), P-Preferred-Identity (if exists), and Remote-Party-ID (if exists)

The IP to IP Inbound Manipulation table provides two configuration areas:

- Matching characteristics (*Rule*) of incoming call, for example, source host name.
- Manipulation operation (*Action*), for example, remove user-defined number of characters from the left of the SIP URI user part.

If the incoming call matches the characteristics of a rule, then its manipulation action is applied.



**Notes:**

- The IP Group table can be used to configure a host name that overwrites the received host name. This manipulation can be done for source or destination IP Groups (see 'Configuring IP Groups' on page 204).
- The IP to IP Inbound Manipulation table can also be configured using the table ini file parameter, IPInboundManipulation or CLI command, configure voip > sbc manipulations ip-inbound-manipulation.

➤ **To configure IP-to-IP inbound manipulation rules:**

1. Open the IP to IP Inbound Manipulation page (**Configuration** tab > **VoIP** menu > **SBC** > **Manipulations SBC** > **IP to IP Inbound**).
2. Click the **Add** button; the following dialog box appears:

**Figure 33-12: IP to IP Inbound Manipulation Page - Add Dialog Box**

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

**IP to IP Inbound Manipulation Parameters Description**

Parameter	Description
<b>Matching Characteristics (Rule)</b>	
Additional Manipulation CLI: is-additional-manipulation	<p>Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it.</p> <ul style="list-style-type: none"> <li>■ <b>[0]</b> No = (Default) Regular manipulation rule (not done in addition to</li> </ul>

Parameter	Description
<b>[IPInboundManipulation_IsAdditionalManipulation]</b>	<p>the rule above it).</p> <ul style="list-style-type: none"> <li><b>[1]</b> Yes = If the above row entry rule matched the call, consider this row entry as a match as well and perform the manipulation specified by this rule.</li> </ul> <p><b>Note:</b> Additional manipulation can only be done on a different SIP URI, source or destination, to the rule configured in the row above as configured by the 'Manipulated URI' parameter (see below).</p>
Manipulation Purpose CLI: purpose <b>[IPInboundManipulation_ManipulationPurpose]</b>	<p>Defines the purpose of the manipulation:</p> <ul style="list-style-type: none"> <li><b>[0]</b> Normal = (Default) Inbound manipulations affect the routing input and source and/or destination number.</li> <li><b>[1]</b> Routing input only = Inbound manipulations affect the routing input only, retaining the original source and destination number.</li> <li><b>[2]</b> Shared Line = Used for the Shared-Line Appearance feature. This manipulation is for registration requests to change the destination number of the secondary extension numbers to the primary extension. For more information, see 'BroadSoft's Shared Phone Line Call Appearance for SBC Survivability' on page 444.</li> </ul>
Source IP Group ID CLI: src-ip-group-id <b>[IPInboundManipulation_SrcIpGroup]</b>	<p>Defines the IP Group from where the incoming INVITE is received.</p> <p>For any IP Group, enter the value "-1".</p>
Source Username Prefix CLI: src-user-name-prefix <b>[IPInboundManipulation_SrcUsernamePrefix]</b>	<p>Defines the prefix of the source SIP URI user name (usually in the From header).</p> <p>For any prefix, enter the asterisk "*" symbol (default).</p> <p><b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659.</p>
Source Host CLI: src-host <b>[IPInboundManipulation_SrcHost]</b>	<p>Defines the source SIP URI host name - full name (usually in the From header). For any host name, enter the asterisk "*" symbol (default).</p>
Destination Username Prefix CLI: dst-user-name-prefix <b>[IPInboundManipulation_DestUsernamePrefix]</b>	<p>Defines the prefix of the destination SIP URI user name (usually in the Request-URI).</p> <p>For any prefix, enter the asterisk "*" symbol (default).</p> <p><b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659.</p>
Destination Host CLI: dst-host <b>[IPInboundManipulation_DestHost]</b>	<p>Defines the destination SIP URI host name - full name (usually in the Request URI).</p> <p>For any host name, enter the asterisk "*" symbol (default).</p>
Request Type CLI: request-type <b>[IPInboundManipulation_RequestType]</b>	<p>Defines the SIP request type to which the manipulation rule is applied.</p> <ul style="list-style-type: none"> <li><b>[0]</b> All = (Default) All SIP messages.</li> <li><b>[1]</b> INVITE = All SIP messages except REGISTER and SUBSCRIBE.</li> <li><b>[2]</b> REGISTER = Only REGISTER messages.</li> <li><b>[3]</b> SUBSCRIBE = Only SUBSCRIBE messages.</li> <li><b>[4]</b> INVITE and REGISTER = All SIP messages except SUBSCRIBE.</li> <li><b>[5]</b> INVITE and SUBSCRIBE = All SIP messages except REGISTER.</li> </ul>

Parameter	Description
Manipulated URI CLI: manipulated-uri <b>[IPInboundManipulation_ManipulatedURI]</b>	Determines whether the source or destination SIP URI user part is manipulated. <ul style="list-style-type: none"> <li><b>[0]</b> Source = (Default) Manipulation is done on the source SIP URI user part.</li> <li><b>[1]</b> Destination = Manipulation is done on the destination SIP URI user part.</li> </ul>
<b>Operation Rule (Action)</b>	
Remove From Left CLI: remove-from-left <b>[IPInboundManipulation_RemoveFromLeft]</b>	Defines the number of digits to remove from the left of the user name prefix. For example, if you enter 3 and the user name is "john", the new user name is "n".
Remove From Right CLI: remove-from-right <b>[IPInboundManipulation_RemoveFromRight]</b>	Defines the number of digits to remove from the right of the user name prefix. For example, if you enter 3 and the user name is "john", the new user name is "j". <b>Note:</b> If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.
Leave From Right CLI: leave-from-right <b>[IPInboundManipulation_LeaveFromRight]</b>	Defines the number of characters that you want retained from the right of the user name. <b>Note:</b> If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.
Prefix to Add CLI: prefix-to-add <b>[IPInboundManipulation_Prefix2Add]</b>	Defines the number or string that you want added to the front of the user name. For example, if you enter 'user' and the user name is "john", the new user name is "userjohn".
Suffix to Add CLI: suffix-to-add <b>[IPInboundManipulation_Suffix2Add]</b>	Defines the number or string that you want added to the end of the user name. For example, if you enter '01' and the user name is "john", the new user name is "john01".

### 33.5.2 Configuring IP-to-IP Outbound Manipulations

The IP to IP Outbound Manipulation page allows you to configure up to 100 manipulation rules for manipulating SIP URI user part (source and destination) of outbound SIP dialog requests. Manipulation rules in the table are located according to the source IP Group, and source and destination host and user prefixes and can be applied to a user-defined SIP request type (e.g., INVITE, OPTIONS, SUBSCRIBE, and /or REGISTER). However, since outbound manipulations are done only after routing, the outbound manipulation rule matching can also be done by destination IP Group.

- Manipulated destination URI user part are performed on the following SIP headers: Request URI, To, and Remote-Party-ID (if exists).
- Manipulated source URI user part are performed on the following SIP headers: From, P-Asserted (if exists), P-Preferred (if exists), and Remote-Party-ID (if exists).

The IP to IP Outbound Manipulation table provides two configuration areas:

- Matching characteristics (*Rule*) of incoming call, for example, source host name.
- Manipulation operation (*Action*), for example, remove user-defined number of characters from the left of the SIP URI user part.

If the incoming call matches the characteristics of a rule, then its manipulation action is applied.

**Notes:**

- Manipulated destination SIP URI user names are done on the following SIP headers: Request URI, To, and Remote-Party-ID (if exists).
- Manipulated source SIP URI user names are done on the following SIP headers: From, P-Asserted (if exists), P-Preferred (if exists), and Remote-Party-ID (if exists)
- SIP URI host name (source and destination) manipulations can also be configured in the IP Group table. These manipulations are simply host name substitutions with the names defined for the source and destination IP Groups respectively.
- The IP to IP Outbound Manipulation table can also be configured using the table ini file parameter, IPOutboundManipulation or CLI command, configure voip > sbc manipulations ip-outbound-manipulation.

➤ **To configure IP-to-IP outbound manipulation rules:**

1. Open the IP to IP Outbound Manipulation page (**Configuration** tab > **VoIP** menu > **SBC > Manipulations SBC > IP to IP Outbound**).
2. Click the **Add** button; the following dialog box appears:

**Figure 33-13: IP to IP Outbound Manipulation Page - Add Dialog Box**

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

**IP to IP Outbound Manipulation Table Parameters Description**

Parameter	Description
<b>Matching Characteristics (Rule)</b>	
Additional Manipulation CLI: is-additional-	Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it.



Parameter	Description
manipulation [IPOutboundManipulation_IsAdditionalManipulation]	<ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) Regular manipulation rule - not done in addition to the rule above it.</li> <li><b>[1]</b> Yes = If the previous table row entry rule matched the call, consider this row entry as a match as well and perform the manipulation specified by this rule.</li> </ul> <p><b>Note:</b> Additional manipulation can only be performed on a different SIP URI (either source or destination) to the rule configured in the row above (configured by the 'Manipulated URI' parameter).</p>
Source IP Group ID CLI: src-ip-group-id [IPOutboundManipulation_SrcIPGroupID]	Defines the IP Group from where the INVITE is received. For any Source IP Group, enter the value -1.
Destination IP Group ID CLI: dst-ip-group-id [IPOutboundManipulation_DestIPGroupID]	Defines the IP Group to where the INVITE is to be sent. For any Destination IP Group, enter the value -1.
Source Username Prefix CLI: src-user-name-prefix [IPOutboundManipulation_SrcUsernamePrefix]	Defines the prefix of the source SIP URI user name (usually in the From header). For any prefix, enter the asterisk "*" symbol (default). <b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659.
Source Host CLI: src-host [IPOutboundManipulation_SrcHost]	Defines the source SIP URI host name - full name (usually in the From header). For any host name, enter the asterisk "*" symbol (default).
Destination Username Prefix CLI: dst-user-name-prefix [IPOutboundManipulation_DestUsernamePrefix]	Defines the prefix of the destination SIP URI user name (usually in the Request-URI). For any prefix, enter the asterisk "*" symbol (default). <b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659.
Destination Host CLI: dst-host [IPOutboundManipulation_DestHost]	Defines the destination SIP URI host name - full name (usually in the Request URI). For any host name, enter the asterisk "*" symbol (default).
Request Type CLI: request-type [IPOutboundManipulation_RequestType]	Defines the SIP request type to which the manipulation rule is applied. <ul style="list-style-type: none"> <li><b>[0]</b> All = (Default) all SIP messages.</li> <li><b>[1]</b> INVITE = All SIP messages except REGISTER and SUBSCRIBE.</li> <li><b>[2]</b> REGISTER = Only SIP REGISTER messages.</li> <li><b>[3]</b> SUBSCRIBE = Only SIP SUBSCRIBE messages.</li> <li><b>[4]</b> INVITE and REGISTER = All SIP messages except SUBSCRIBE.</li> <li><b>[5]</b> INVITE and SUBSCRIBE = All SIP messages except REGISTER.</li> </ul>
ReRoute IP Group ID CLI: re-route-ip-group-id [IPOutboundManipulation_ReRouteIPGroupID]	Defines the IP Group that initiated (sent) the SIP redirect response (e.g., 3xx) or REFER message. This parameter is typically used for re-routing requests (e.g., INVITEs) when interworking is required for SIP 3xx redirect responses or REFER messages. The default is -1 (i.e., not configured). <b>Notes:</b>



Parameter	Description
	<ul style="list-style-type: none"> <li>This parameter functions together with the 'Call Trigger' parameter (see below).</li> <li>For more information on interworking of SIP 3xx redirect responses or REFER messages, see 'Interworking SIP 3xx Redirect Responses' on page 436 and 'Interworking SIP REFER Messages' on page 439, respectively.</li> </ul>
Call Trigger CLI: trigger <b>[IPOutboundManipulation_Trigger]</b>	<p>Defines the reason (i.e, trigger) for the re-routing of the SIP request:</p> <ul style="list-style-type: none"> <li><b>[0]</b> Any = (Default) Re-routed for all scenarios (re-routes and non-re-routes).</li> <li><b>[1]</b> 3xx = Re-routed if it triggered as a result of a SIP 3xx response.</li> <li><b>[2]</b> REFER = Re-routed if it triggered as a result of a REFER request.</li> <li><b>[3]</b> 3xx or REFER = Applies to options <b>[1]</b> and <b>[2]</b>.</li> <li><b>[4]</b> Initial only = Regular requests that the device forwards to a destination. In other words, re-routing of requests triggered by the receipt of REFER or 3xx does not apply.</li> </ul>
Manipulated URI CLI: manipulated-uri <b>[IPOutboundManipulation_IsAdditionalManipulation]</b>	<p>Determines whether the source or destination SIP URI user part is manipulated.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Source = (Default) Manipulation is done on the source SIP URI user part.</li> <li><b>[1]</b> Destination = Manipulation is done on the destination SIP URI user part.</li> </ul>
<b>Operation Manipulation Rule (Action)</b>	
Remove From Left CLI: remove-from-left <b>[IPOutboundManipulation_RemoveFromLeft]</b>	<p>Defines the number of digits to remove from the left of the user name prefix. For example, if you enter 3 and the user name is "john", the new user name is "n".</p>
Remove From Right CLI: remove-from-right <b>[IPOutboundManipulation_RemoveFromRight]</b>	<p>Defines the number of digits to remove from the right of the user name prefix. For example, if you enter 3 and the user name is "john", the new user name is "j".</p>
Leave From Right CLI: leave-from-right <b>[IPOutboundManipulation_LeaveFromRight]</b>	<p>Defines the number of characters that you want retained from the right of the user name.</p>
Prefix to Add CLI: prefix-to-add <b>[IPOutboundManipulation_Prefix2Add]</b>	<p>Defines the number or string that you want added to the front of the user name. For example, if you enter 'user' and the user name is "john", the new user name is "userjohn".</p>
Suffix to Add CLI: suffix-to-add <b>[IPOutboundManipulation_Suffix2Add]</b>	<p>Defines the number or string that you want added to the end of the user name. For example, if you enter '01' and the user name is "john", the new user name is "john01".</p>
Privacy Restriction Mode CLI: privacy-restriction-mode <b>[IPOutboundManipulation_PrivacyRestrictionMode]</b>	<p>Determines user privacy handling (i.e., restricting source user identity in outgoing SIP dialogs).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Transparent = (Default) No intervention in SIP privacy.</li> <li><b>[1]</b> Don't change privacy = The user identity remains the same as in the incoming SIP dialog. If a restricted number exists, the restricted presentation is normalized as follows: <ul style="list-style-type: none"> <li>✓ From URL header: anonymous@anonymous.invalid.</li> </ul> </li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>✓ If a P-Asserted-Identity header exists (either in the incoming SIP dialog or added by the device), a Privacy header is added with the value "id".</li> <li>▪ <b>[2] Restrict</b> = The user identity is restricted (the restricted presentation is as mentioned above).</li> <li>▪ <b>[3] Remove Restriction</b> = The device attempts to reveal the user identity by setting user values in the From header and removing the privacy "id" value if the Privacy header exists.</li> </ul> <p>If the From header user is anonymous, the value is taken from the P-Preferred-Identity, P-Asserted-Identity, or Remote-Party-ID header (if exists).</p> <p>The device identifies an incoming user as restricted if one of the following exists:</p> <ul style="list-style-type: none"> <li>▪ From header user is anonymous.</li> <li>▪ P-Asserted-Identity and Privacy headers contain the value "id".</li> </ul> <p><b>Note:</b> All restriction logic is performed after the user number has been manipulated.</p>

# Part VII

## Cloud Resilience Package Application



## 34 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 similar to the SAS application. 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 headquarters. The device maintains call continuity even if a failure occurs in communication with the hosted IP PBX. It does this by using its Call Survivability feature, enabling the branch users to call one another or make external calls through the device's PSTN gateway interface (if configured).

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 2: Key Features**

Survivability	Quality of Experience/Service	Security
<ul style="list-style-type: none"><li>■ PSTN fallback*</li><li>■ WAN redundancy</li><li>■ Local mode</li><li>■ High availability*</li><li>■ Emergency calling (E911)</li></ul>	<ul style="list-style-type: none"><li>■ QoE monitoring</li><li>■ Call Admission Control</li><li>■ SLA fulfillment</li><li>■ SIP mediation</li><li>■ Media transcoding</li><li>■ Test call agent</li></ul>	<ul style="list-style-type: none"><li>■ Layer 3 to 7 protection</li><li>■ Media encryption</li><li>■ Call control encryption</li><li>■ NAT traversal</li><li>■ Topology hiding</li></ul>

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 such as for IP addresses to get the device up and running and deployed in the network.

## Reader's Notes

## 35 CRP Configuration

This section describes configuration specific to the CRP application. As CRP has similar functionality to the SBC application, for configuration common to the SBC, which is not covered in this section, see the following SBC sections:

- Configuring General Settings (see Configuring General Settings on page 451)
- Configuring Admission Control (see Configuring Admission Control on page 452)
- Configuring Allowed Coder Groups (see Configuring Allowed Coder Groups on page 454)
- Configuring Classification Rules (see Configuring Classification Rules on page 456)
- Configuring Condition Rules (see Configuring Condition Rules on page 461)
- Configuring SBC IP-to-IP Routing (see Configuring SBC IP-to-IP Routing on page 462)
- Configuring Alternative Routing Reasons (see Configuring Alternative Routing Reasons on page 468)
- Configuring IP-to-IP Inbound Manipulations (see Configuring IP-to-IP Inbound Manipulations on page 471)
- Configuring IP-to-IP Outbound Manipulations (see Configuring IP-to-IP Outbound Manipulations on page 474)



**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".

### 35.1 Enabling the CRP Application

The procedure below describes how to enable the CRP application.



**Note:** For CRP support, the device must be installed with the relevant Software License Key. This License Key must also be defined with the required number of call sessions.

➤ **To enable the CRP application:**

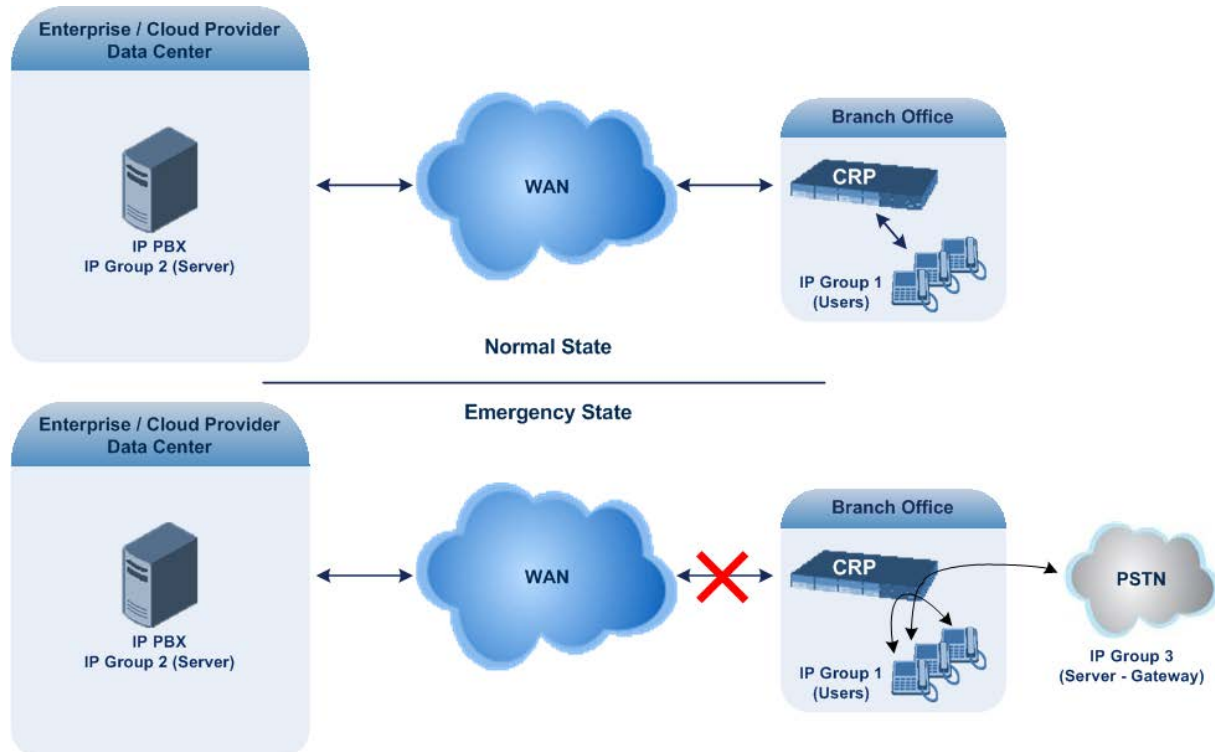
1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).
2. From the 'Enable CRP Application' drop-down list, select **Enable**.
3. Save (burn) the changes to the device's flash memory with a device reset (see Saving Configuration on 532).

## 35.2 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 routes the calls between the branch users themselves. If this fails, it routes the calls to the PSTN (if employed).

**Figure 14: 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.

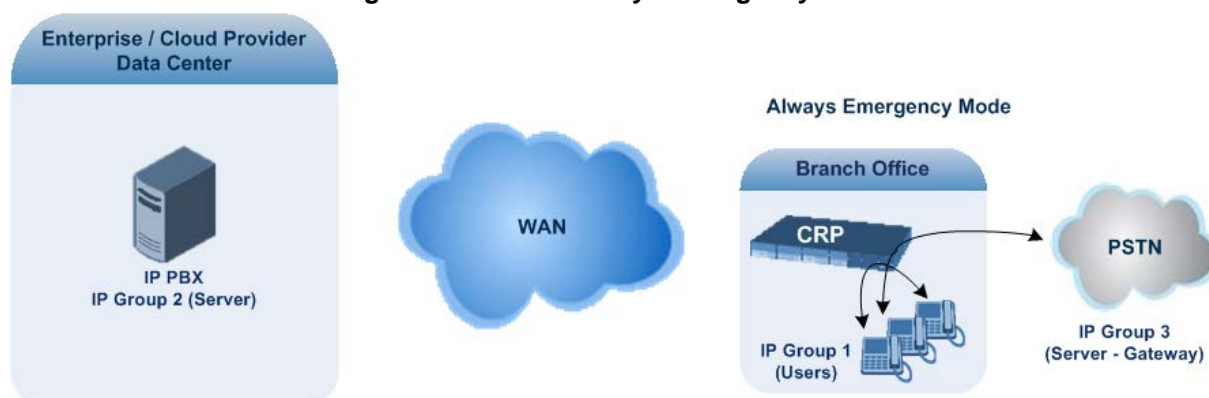


**Note:** SIP REGISTER and OPTIONS requests are terminated at the CRP.



- **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 15: CRP in Always Emergency Mode



➤ **To configure the Call Survivability mode:**

1. Open the General Settings page (**Configuration** tab > **VoIP** menu > **CRP** > **General Settings**).
2. From the 'CRP Survivability Mode' drop-down list, select the required mode.
3. Click **Submit**.

### 35.3 Pre-Configured IP Groups

The IP Group table for CRP is pre-configured with the following IP Groups:

Table 3: Pre-configured IP Groups in the IP Group 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 headquarters)
- **"Gateway" IP Group:** 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 486).



**Notes:**

- 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 Group table and for a description of its parameters, see Configuring IP Groups on page 204.

## 35.4 Pre-Configured IP-to-IP Routing Rules

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 484.



### Notes:

- 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 on page 462.

**Table 4: Pre-Configured Rules in IP-to-IP Routing Table**

Mode	Index	Source IP Group ID	Request Type	Destination Type	Destination IP Group ID	Destination Address	Alternative Route Options
Normal	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	3	All	IP Group	2	-	Route Row
	8	3	All	IP Group	1	-	Alternative
Always Emergency	1	*	OPTIONS	Dest Address	-	Internal	Route Row
	2	*	REGISTER	Dest Address	-	Internal	Route Row
	4	1	All	IP Group	1	-	Route Row
	5	1	All	IP Group	3	-	Alternative
	8	3	All	IP Group	1	-	Route Row
Auto Answer to Registrations	1	*	OPTIONS	Dest Address	-	Internal	Route Row
	2	*	REGISTER	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	3	All	IP Group	2	-	Route Row
	8	3	All	IP Group	1	-	Alternative

# Part VIII

## Stand-Alone Survivability Application



## 36 SAS Overview

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

**Notes:**

- The SAS application is available only if the device is installed with the SAS Software License Key.
- Throughout this section, the term *user agent* (UA) refers to the enterprise's LAN phone user (i.e., SIP telephony entities such as IP phones).
- Throughout this section, the term *proxy* or *proxy server* refers to the enterprise's centralized IP Centrex or IP-PBX.
- Throughout this section, the term SAS refers to the SAS application running on the device.

### 36.1 SAS Operating Modes

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

- **Outbound Proxy:** In this mode, SAS receives SIP REGISTER requests from the enterprise's UAs and forwards these requests to the external proxy (i.e., outbound proxy). When a connection with the external proxy fails, SAS enters SAS emergency state and serves as a proxy, by handling internal call routing for the enterprise's UAs - routing calls between UAs and if setup, routing calls between UAs and the PSTN. For more information, see 'SAS Outbound Mode' on page 490.
- **Redundant Proxy:** In this mode, the enterprise's UAs register with the external proxy and establish calls directly through the external proxy, without traversing SAS (or the device per se'). Only when connection with the proxy fails, do the UAs register with SAS, serving now as the UAs redundant proxy. SAS then handles the calls between UAs, and between the UAs and the PSTN (if setup). This mode is operational only during SAS in emergency state. This mode can be implemented, for example, for proxies that accept only SIP messages that are sent directly from the UAs. For more information, see 'SAS Redundant Mode' on page 491.



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

## 36.1.1 SAS Outbound Mode

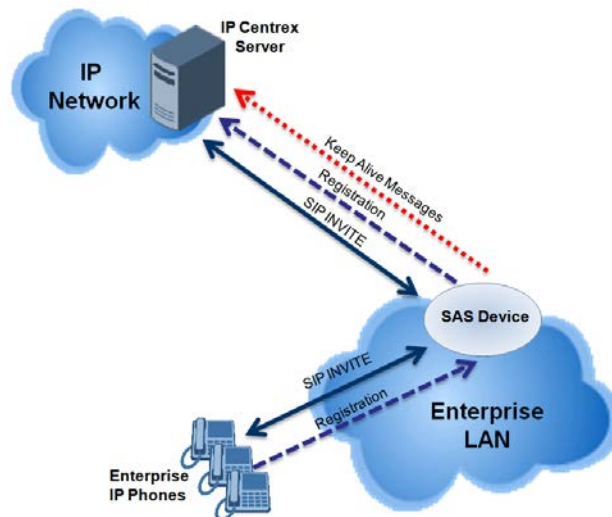
This section describes the SAS outbound mode, which includes the following states:

- Normal state (see 'Normal State' on page 490)
- Emergency state (see 'Emergency State' on page 490)

### 36.1.1.1 Normal State

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

**Figure 36-1: SAS Outbound Mode in Normal State (Example)**



### 36.1.1.2 Emergency State

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



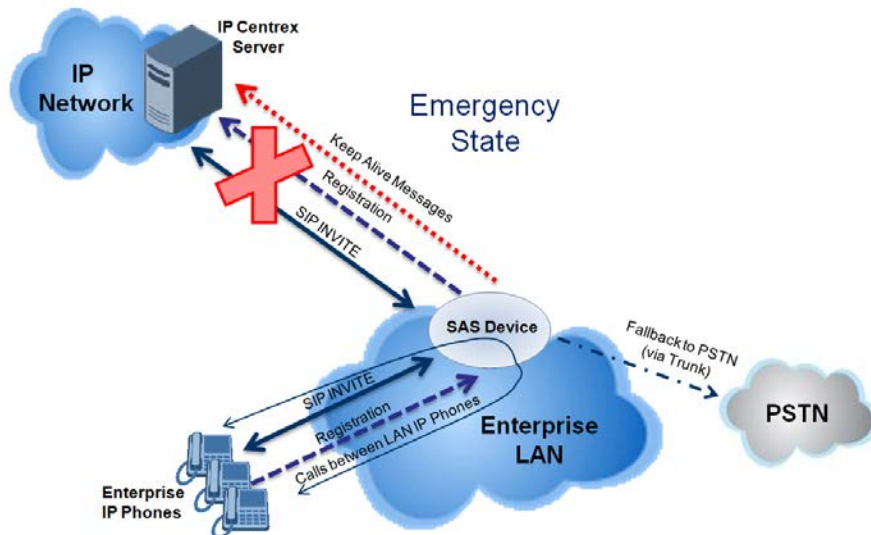
**Note:** SAS can also enter Emergency state if no response is received from the proxy for sent OPTIONS, INVITE, or REGISTER messages. To configure this, set the SASEnteringEmergencyMode parameter to 1.

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

The routing logic of SAS in emergency state is described in detail in 'SAS Routing in Emergency State' on page 495.

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

Figure 36-2: SAS Outbound Mode in Emergency State (Example)



When emergency state is active, SAS continuously attempts to communicate with the external proxy, using keep-alive SIP OPTIONS. Once connection to the proxy returns, the device exits SAS emergency state and returns to SAS normal state, as explained in 'Exiting Emergency and Returning to Normal State' on page 492.

### 36.1.2 SAS Redundant Mode

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

This mode is operational only during SAS in emergency state.

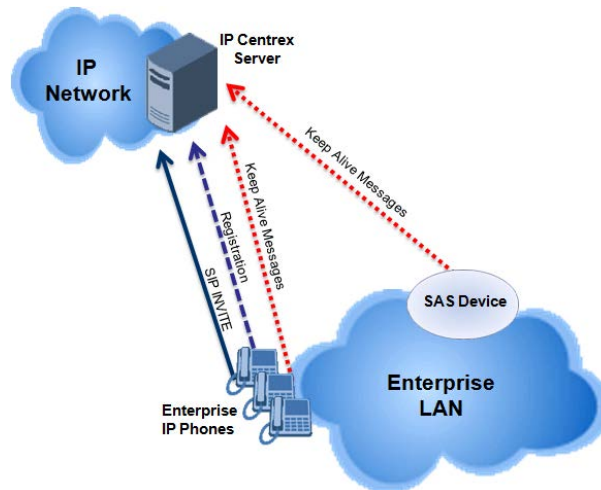


**Note:** In this SAS deployment, the UAs (e.g., IP phones) must support configuration for primary and secondary proxy servers (i.e., proxy redundancy), as well as homing. Homing allows the UAs to switch back to the primary server from the secondary proxy once the connection to the primary server returns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

### 36.1.2.1 Normal State

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

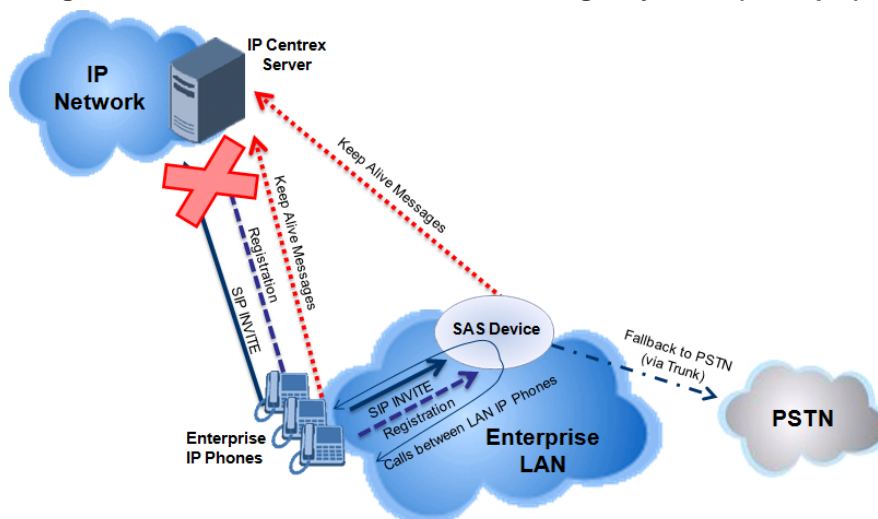
**Figure 36-3: SAS Redundant Mode in Normal State (Example)**



### 36.1.2.2 Emergency State

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

**Figure 36-4: SAS Redundant Mode in Emergency State (Example)**



### 36.1.2.3 Exiting Emergency and Returning to Normal State

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

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

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



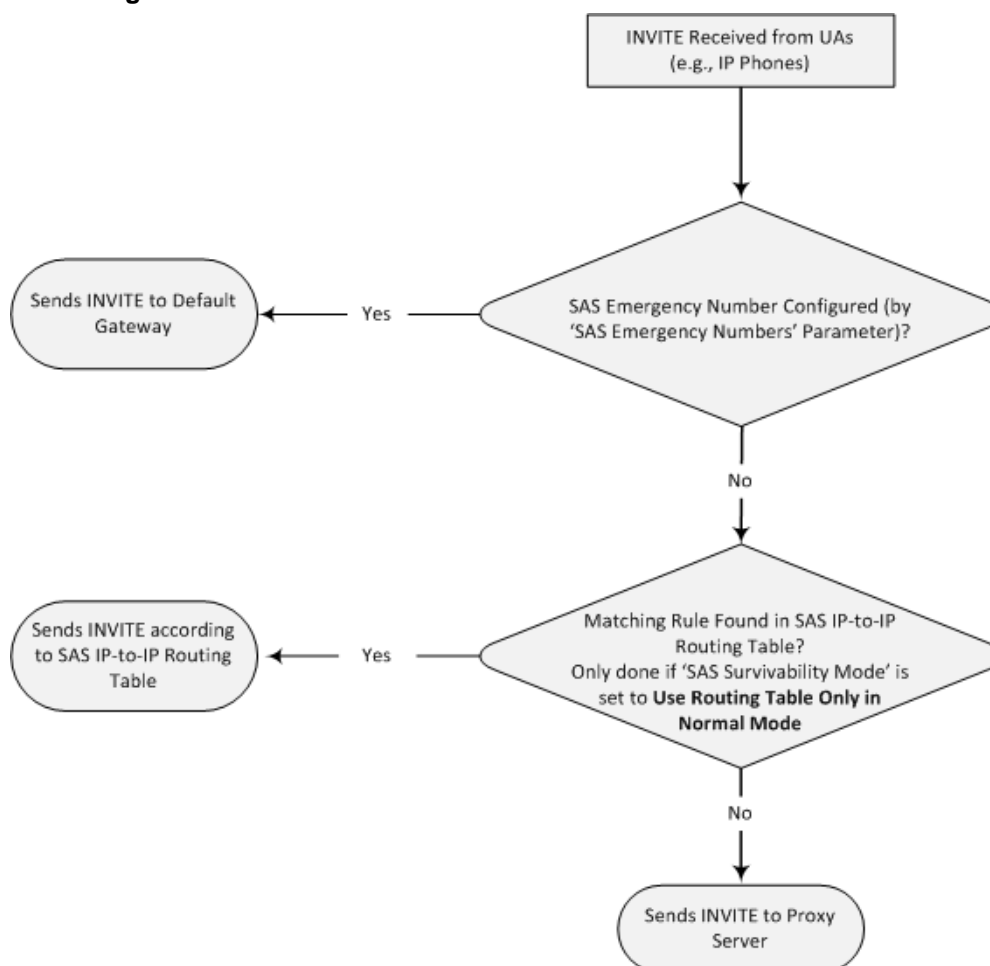
## 36.2 SAS Routing

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

### 36.2.1 SAS Routing in Normal State

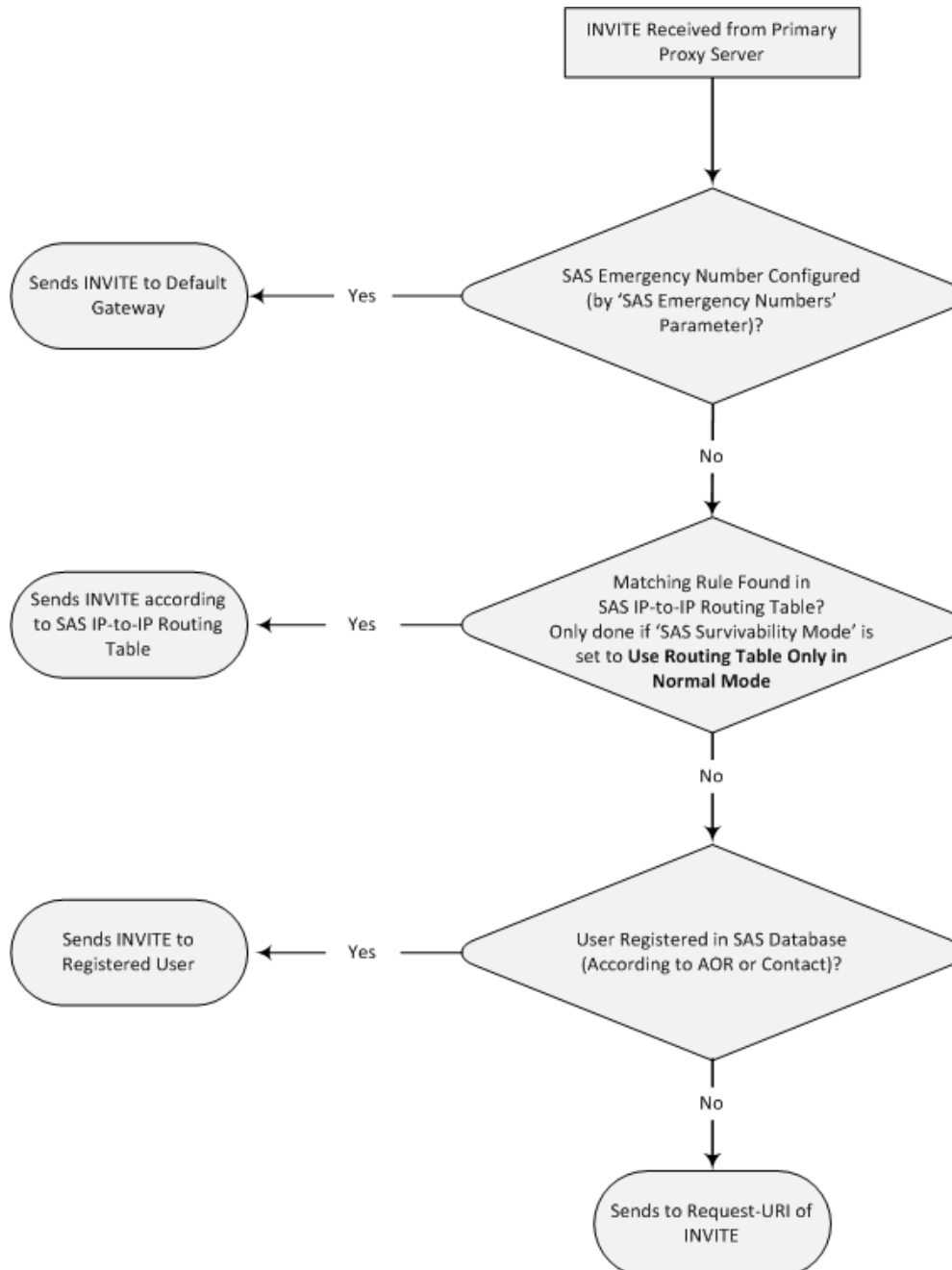
The flowchart below displays the routing logic for SAS in normal state for INVITE messages received from UAs:

**Figure 36-5: Flowchart of INVITE from UA's in SAS Normal State**



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

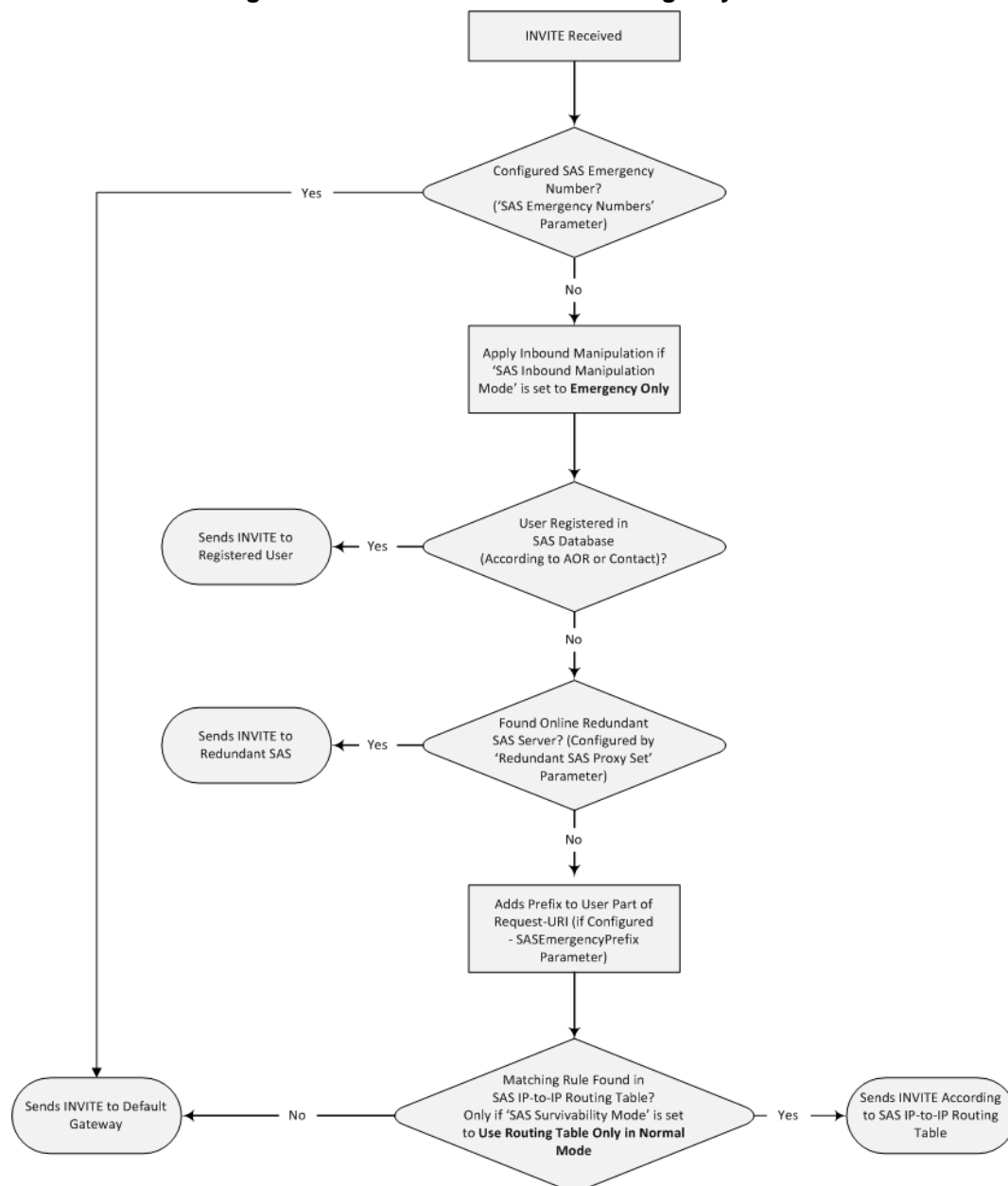
**Figure 36-6: Flowchart of INVITE from Primary Proxy in SAS Normal State**



## 36.2.2 SAS Routing in Emergency State

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

**Figure 36-7: Flowchart for SAS Emergency State**



## Reader's Notes

## 37 SAS Configuration

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

The SAS configuration includes the following:

- General SAS configuration that is common to all SAS deployment types (see 'General SAS Configuration' on page 497)
- SAS outbound mode (see 'Configuring SAS Outbound Mode' on page 500)
- SAS redundant mode (see 'Configuring SAS Redundant Mode' on page 500)
- Gateway and SAS applications deployed together (see 'Configuring Gateway Application with SAS' on page 501)
- Optional, advanced SAS features (see 'Advanced SAS Configuration' on page 504)

### 37.1 General SAS Configuration

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

#### 37.1.1 Enabling the SAS Application

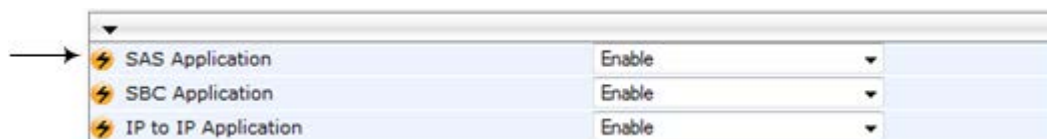
Before you can configure SAS, you need to enable the SAS application on the device. Once enabled, the **SAS** menu and related pages appear in the device's Web interface.



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

➤ **To enable the SAS application:**

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



3. Click **Submit**.
4. Save the changes to the flash memory with a device reset.

#### 37.1.2 Configuring Common SAS Parameters

The procedure below describes how to configure SAS settings that are common to all SAS modes. This includes various SAS parameters as well as configuring the Proxy Set for the SAS proxy (if required). The SAS Proxy Set ID defines the address of the UAs' external proxy.

➤ **To configure common SAS settings:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. Define the port used for sending and receiving SAS messages. This can be any of the following port types:
  - UDP port - defined in the 'SAS Local SIP UDP Port' field
  - TCP port - defined in the 'SAS Local SIP TCP Port' field
  - TLS port - defined in the 'SAS Local SIP TLS Port' field

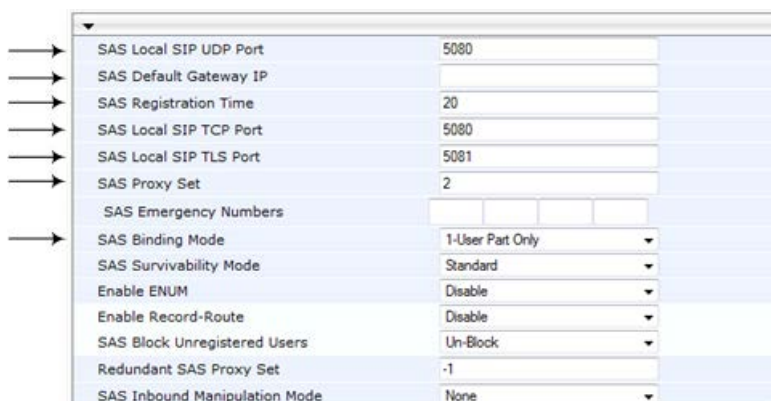


**Note:** This SAS port must be different than the device's local gateway port (i.e., that defined for the 'SIP UDP/TCP/TLS Local Port' parameter in the SIP General Parameters page - **Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

3. In the 'SAS Default Gateway IP' field, define the IP address and port (in the format *x.x.x.x:port*) of the device (i.e., Gateway application). Note that the port of the device is defined by the parameter 'SIP UDP Local Port' (refer to the note in Step 2 above).
4. In the 'SAS Registration Time' field, define the value for the SIP Expires header, which is sent in the 200 OK response to an incoming REGISTER message when SAS is in emergency state.
5. From the 'SAS Binding Mode' drop-down list, select the database binding mode:
  - **0-URI:** If the incoming AOR in the REGISTER request uses a 'tel:' URI or 'user=phone', the binding is done according to the Request-URI user part only. Otherwise, the binding is done according to the entire Request-URI (i.e., user and host parts - user@host).
  - **1-User Part Only:** Binding is done according to the user part only.

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

**Figure 37-1: Configuring Common Settings**



SAS Local SIP UDP Port	5080
SAS Default Gateway IP	
SAS Registration Time	20
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	2
SAS Emergency Numbers	
SAS Binding Mode	1-User Part Only
SAS Survivability Mode	Standard
Enable ENUM	Disable
Enable Record-Route	Disable
SAS Block Unregistered Users	Un-Block
Redundant SAS Proxy Set	-1
SAS Inbound Manipulation Mode	None

6. In the 'SAS Proxy Set' field, enter the Proxy Set used for SAS. The SAS Proxy Set must be defined only for the following SAS modes:

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

If you define a SAS Proxy Set ID, you must configure the Proxy Set as described in Step 8 below.

7. Click **Submit** to apply your settings.
8. If you defined a SAS Proxy Set ID in Step 6 above, then you must configure the SAS Proxy Set ID:
  - a. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Networks** > **Proxy Set Table**).
  - b. From the 'Proxy Set ID' drop-down list, select the required Proxy Set ID.



**Notes:**

- The selected Proxy Set ID number must be the same as that specified in the 'SAS Proxy Set' field in the 'SAS Configuration page (see Step 6).
- Do not use Proxy Set ID 0.

- c. In the 'Proxy Address' field, enter the IP address of the external proxy server.
- d. From the 'Enable Proxy Keep Alive' drop-down list, select **Using Options**. This instructs the device to send SIP OPTIONS messages to the proxy for the keep-alive mechanism.

**Figure 37-2: Defining SAS Proxy Server**

	Proxy Address	Transport Type
1	10.15.4.52	TLS
2		
3		
4		
5		

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

- e. Click **Submit** to apply your settings.

## 37.2 Configuring SAS Outbound Mode

This section describes how to configure the SAS outbound mode. These settings are in addition to the ones described in 'Configuring Common SAS Parameters' on page 497.



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

➤ **To configure SAS outbound mode:**

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

## 37.3 Configuring SAS Redundant Mode

This section describes how to configure the SAS redundant mode. These settings are in addition to the ones described in 'Configuring Common SAS Parameters' on page 497.



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

➤ **To configure SAS redundant mode:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the 'SAS Survivability Mode' drop-down list, select one of the following, depending on whether the UAs support homing (i.e., they always attempt to operate with the primary proxy, and if using the redundant proxy, they switch back to the primary proxy whenever it's available):
  - **UAs support homing:** Select **Always Emergency**. This is because SAS does not need to communicate with the primary proxy of the UAs; SAS serves only as the redundant proxy of the UAs. When the UAs detect that their primary proxy is available, they automatically resume communication with it instead of with SAS.
  - **UAs do not support homing:** Select **Ignore REGISTER**. SAS uses the keep-alive mechanism to detect availability of the primary proxy (defined by the SAS Proxy Set). If the connection with the primary proxy resumes, SAS ignores the messages received from the UAs, forcing them to send their messages directly to the primary proxy.
3. Click **Submit**.



## 37.4 Configuring Gateway Application with SAS

If you want to run both the Gateway and SAS applications on the device, the configuration described in this section is required. The configuration steps depend on whether the Gateway application is operating with SAS in outbound mode or SAS in redundant mode.



**Note:** The Gateway application must use the same SAS operation mode as the SIP UAs. For example, if the UAs use the SAS application as a redundant proxy (i.e., SAS redundancy mode), then the Gateway application must do the same.

### 37.4.1 Gateway with SAS Outbound Mode

The procedure below describes how to configure the Gateway application with SAS outbound mode.

➤ **To configure Gateway application with SAS outbound mode:**

1. Define the proxy server address for the Gateway application:
  - a. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Proxy & Registration**).
  - b. From the 'Use Default Proxy' drop-down list, select **Yes**.

**Figure 37-3: Enabling Proxy Server for Gateway Application**

- c. Click **Submit**.
- d. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets** Table).
- e. From the 'Proxy Set ID' drop-down list, select **0**.
- f. In the first 'Proxy Address' field, enter the IP address and port of the device (in the format `x.x.x.x:port`). This is the port as defined in the 'SAS Local UDP/TCP/TLS Port' field (see 'Configuring Common SAS Parameters' on page 497).

Figure 37-4: Defining Proxy Server for Gateway Application

	Proxy Address	Transport Type
1	202.10.13.1:5080	UDP
2		
3		
4		
5		

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

- g. Click **Submit**.
2. Disable use of user=phone in SIP URL:
  - a. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).
  - b. From the 'Use user=phone in SIP URL' drop-down list, select **No**. This instructs the Gateway application not to use *user=phone* in the SIP URL and therefore, REGISTER and INVITE messages use SIP URI. (By default, REGISTER messages are sent with *sip uri* and INVITE messages with *tel uri*.)

Figure 37-5: Disabling user=phone in SIP URL

SIP General	
NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Disable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	No Fax
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	UDP
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5060
Use user=phone in SIP URL	No

- c. Click **Submit**.

## 37.4.2 Gateway with SAS Redundant Mode

The procedure below describes how to configure the Gateway application with SAS redundant mode.

➤ **To configure Gateway application with SAS redundant mode:**

1. Define the proxy servers for the Gateway application:
  - a. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Proxy & Registration**).
  - b. From the 'Use Default Proxy' drop-down list, select **Yes**.

**Figure 37-6: Enabling Proxy Server for Gateway Application**

Use Default Proxy: Yes

Proxy Set Table: [button]

Proxy Name: [text field]

- c. Click **Submit**.
- d. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).
- e. From the 'Proxy Set ID' drop-down list, select **0**.
- f. In the first 'Proxy Address' field, enter the IP address of the external proxy server.
- g. In the second 'Proxy Address' field, enter the IP address and port of the device (in the format *x.x.x.x:port*). This is the same port as defined in the 'SAS Local UDP/TCP/TLS Port' field (see 'Configuring Common SAS Parameters' on page 497).
- h. From the 'Proxy Redundancy Mode' drop-down list, select **Homing**.

**Figure 37-7: Defining Proxy Servers for Gateway Application**

Proxy Set ID: 0

	Proxy Address	Transport Type
1	202.10.13.1:5080	UDP
2	10.13.4.1	UDP
3		
4		
5		

Enable Proxy Keep Alive: Using Options

Proxy Keep Alive Time: 60

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Proxy Redundancy Mode: Homing

SRD Index: 0

Classification Input: IP only

- i. Click **Submit**.
2. Disable the use of *user=phone* in the SIP URL:
  - a. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).
  - b. From the 'Use user=phone in SIP URL' drop-down list, select **No**. This instructs the Gateway application not to use *user=phone* in SIP URL and therefore, REGISTER and INVITE messages use SIP URI. (By default, REGISTER messages are sent with *sip uri* and INVITE messages with *tel uri*.)
  - c. Click **Submit**.

## 37.5 Advanced SAS Configuration

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

### 37.5.1 Manipulating URI user part of Incoming REGISTER

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

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

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

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

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

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

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

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

#### ➤ To manipulate incoming Request-URI user part of REGISTER message:

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

Figure 37-8: Manipulating User Part in Incoming REGISTER

SAS Local SIP UDP Port	5080
SAS Default Gateway IP	10.0.0.2:5080
SAS Registration Time	20
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	0
SAS Emergency Numbers	
SAS Binding Mode	0-URI
SAS Survivability Mode	Always Emergency
Enable ENUM	Disable
Enable Record-Route	Disable
SAS Block Unregistered Users	Un-Block
Redundant SAS Proxy Set	-1
SAS Inbound Manipulation Mode	None

SAS Registration Manipulation	
Remove From Right	Leave From Right
0	4

SAS Routing

SAS Routing Table

3. Click **Submit**.



#### Notes:

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


## 37.5.2 Manipulating Destination Number of Incoming INVITE

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

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

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

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

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the 'SAS Inbound Manipulation Mode' (*SASInboundManipulationMode*) drop-down list, select **Emergency Only**.
3. Click **Submit**; the **SAS Inbound Manipulation Mode Table**  button appears on the page.
4. Click this button to open the IP to IP Inbound Manipulation page.
5. Add your SAS manipulation rule as required. See the table below for descriptions of the parameters.
6. Click **Submit** to save your changes.



**Notes:**

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

**SAS IP to IP Inbound Manipulation Parameters**

Parameter	Description
<b>Matching Characteristics (Rule)</b>	
Additional Manipulation CLI: is-additional-manipulation <b>[IPInboundManipulation_IsAdditionalManipulation]</b>	<p>Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No = (Default) Regular manipulation rule (not done in addition to the rule above it).</li> <li>▪ <b>[1]</b> Yes = If the above row entry rule matched the call, consider this row entry as a match as well and perform the manipulation specified by this rule.</li> </ul> <p><b>Note:</b> Additional manipulation can only be done on a different SIP URI, source or destination, to the rule configured in the row above as configured by the 'Manipulated URI' parameter (see below).</p>
Manipulation Purpose CLI: purpose <b>[IPInboundManipulation_ManipulationPurpose]</b>	<p>Defines the purpose of the manipulation:</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Normal = (Default) Inbound manipulations affect the routing input and source and/or destination number.</li> <li>▪ <b>[1]</b> Routing input only = Inbound manipulations affect the routing input only, retaining the original source and destination number.</li> <li>▪ <b>[2]</b> Shared Line = Used for the Shared-Line Appearance feature. This manipulation is for registration requests to change the destination number of the secondary extension numbers to the primary extension. For more information, see 'BroadSoft's Shared Phone Line Call Appearance for SBC Survivability' on page 444.</li> </ul>
Source IP Group ID CLI: src-ip-group-id <b>[IPInboundManipulation_SrcIpGroup]</b>	<p>Defines the IP Group from where the incoming INVITE is received. For any IP Group, enter the value "-1".</p>



Parameter	Description
Source Username Prefix CLI: src-user-name-prefix <b>[IPInboundManipulation_SrcUsernamePrefix]</b>	Defines the prefix of the source SIP URI user name (usually in the From header). For any prefix, enter the asterisk "*" symbol (default). <b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659.
Source Host CLI: src-host <b>[IPInboundManipulation_SrcHost]</b>	Defines the source SIP URI host name - full name (usually in the From header). For any host name, enter the asterisk "*" symbol (default).
Destination Username Prefix CLI: dst-user-name-prefix <b>[IPInboundManipulation_DestUsernamePrefix]</b>	Defines the prefix of the destination SIP URI user name (usually in the Request-URI). For any prefix, enter the asterisk "*" symbol (default). <b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659.
Destination Host CLI: dst-host <b>[IPInboundManipulation_DestHost]</b>	Defines the destination SIP URI host name - full name (usually in the Request URI). For any host name, enter the asterisk "*" symbol (default).
Request Type CLI: request-type <b>[IPInboundManipulation_RequestType]</b>	Defines the SIP request type to which the manipulation rule is applied. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> All = (Default) All SIP messages.</li> <li>▪ <b>[1]</b> INVITE = All SIP messages except REGISTER and SUBSCRIBE.</li> <li>▪ <b>[2]</b> REGISTER = Only REGISTER messages.</li> <li>▪ <b>[3]</b> SUBSCRIBE = Only SUBSCRIBE messages.</li> <li>▪ <b>[4]</b> INVITE and REGISTER = All SIP messages except SUBSCRIBE.</li> <li>▪ <b>[5]</b> INVITE and SUBSCRIBE = All SIP messages except REGISTER.</li> </ul>
Manipulated URI CLI: manipulated-uri <b>[IPInboundManipulation_ManipulatedURI]</b>	Determines whether the source or destination SIP URI user part is manipulated. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Source = (Default) Manipulation is done on the source SIP URI user part.</li> <li>▪ <b>[1]</b> Destination = Manipulation is done on the destination SIP URI user part.</li> </ul>
<b>Operation Rule (Action)</b>	
Remove From Left CLI: remove-from-left <b>[IPInboundManipulation_RemoveFromLeft]</b>	Defines the number of digits to remove from the left of the user name prefix. For example, if you enter 3 and the user name is "john", the new user name is "n".
Remove From Right CLI: remove-from-right <b>[IPInboundManipulation_RemoveFromRight]</b>	Defines the number of digits to remove from the right of the user name prefix. For example, if you enter 3 and the user name is "john", the new user name is "j". <b>Note:</b> If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.
Leave From Right CLI: leave-from-right <b>[IPInboundManipulation_LeaveFromRight]</b>	Defines the number of characters that you want retained from the right of the user name. <b>Note:</b> If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.

Parameter	Description
Prefix to Add CLI: prefix-to-add <b>[IPInboundManipulation_Prefix2Add]</b>	Defines the number or string that you want added to the front of the user name. For example, if you enter 'user' and the user name is "john", the new user name is "userjohn".
Suffix to Add CLI: suffix-to-add <b>[IPInboundManipulation_Suffix2Add]</b>	Defines the number or string that you want added to the end of the user name. For example, if you enter '01' and the user name is "john", the new user name is "john01".

### 37.5.3 SAS Routing Based on IP-to-IP Routing Table

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

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

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

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


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

- a. Sends the request according to rules configured in the IP-to-IP Routing table.
- b. If no matching routing rule exists, the device sends the request according to its SAS registration database.
- c. If no routing rule is located in the database, the device sends the request according to the Request-URI header.

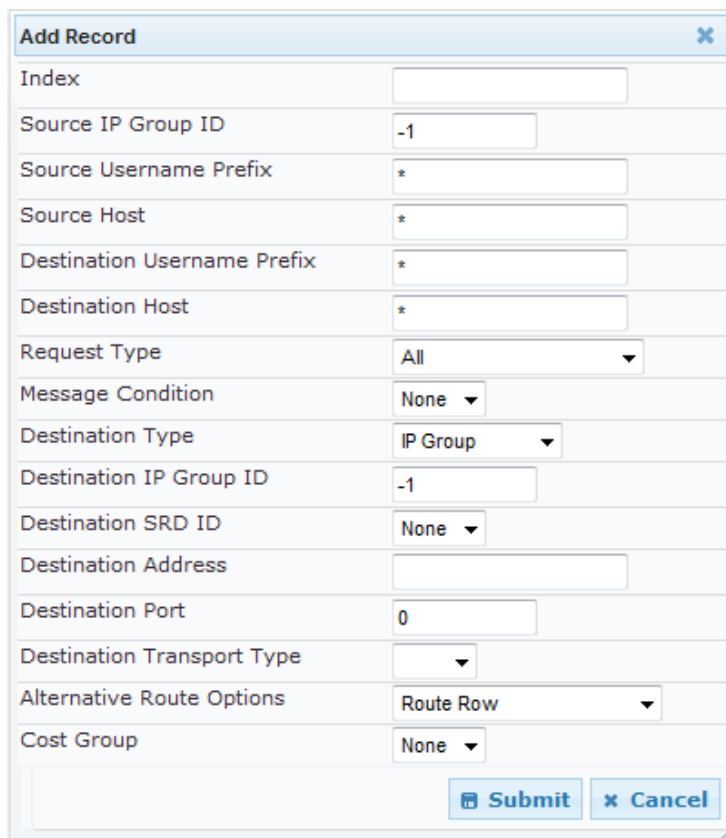


**Note:** The IP-to-IP Routing table can also be configured using the table *ini* file parameter, IP2IPRouting (see 'Configuration Parameters Reference' on page 661) or CLI command, configure voip/sbc routing ip2ip-routing.

#### ➤ To configure the IP-to-IP Routing table for SAS:

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



**Figure 37-9: Add Record Dialog Box of SAS IP2IP Routing Page**


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

- Index: Text input field.
- Source IP Group ID: Text input field with value '-1'.
- Source Username Prefix: Text input field with value '\*'.
- Source Host: Text input field with value '\*'.
- Destination Username Prefix: Text input field with value '\*'.
- Destination Host: Text input field with value '\*'.
- Request Type: Dropdown menu with value 'All'.
- Message Condition: Dropdown menu with value 'None'.
- Destination Type: Dropdown menu with value 'IP Group'.
- Destination IP Group ID: Text input field with value '-1'.
- Destination SRD ID: Dropdown menu with value 'None'.
- Destination Address: Text input field.
- Destination Port: Text input field with value '0'.
- Destination Transport Type: Dropdown menu.
- Alternative Route Options: Dropdown menu with value 'Route Row'.
- Cost Group: Dropdown menu with value 'None'.

At the bottom right, there are 'Submit' and 'Cancel' buttons.

3. Configure the rule according to the table below.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 532.



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

- 'Source IP Group ID'
- 'Destination IP Group ID'
- 'Destination SRD ID'
- 'Alternative Route Options'

#### SAS IP-to-IP Routing Table Parameters

Parameter	Description
<b>Matching Characteristics</b>	
Source IP Group ID [IP2IPRouting_SrcIPGroupID] CLI: src-ip-group-id	Selects the IP Group from where the IP-to-IP call originated. Typically, the IP Group of an incoming SIP dialog is determined (or classified) using the 'Classification' table (see Configuring Classification Rules on page 456). If not used (i.e., any IP Group), simply leave the field empty. The default is -1.
Source Username Prefix [IP2IPRouting_SrcUsernamePrefix] CLI: src-user-name-	Defines the prefix of the user part of the incoming SIP dialog's source URI (usually the From URI). You can use special notations for denoting the prefix. For example, to denote any prefix, use the asterisk (*) symbol; to denote calls without a user part in the URI, use the \$ sign. For

Parameter	Description
prefix	available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659. The default is * (i.e., any prefix).
Source Host <b>[IP2IPRouting_SrcHost]</b> CLI: src-host	Defines the host part of the incoming SIP dialog's source URI (usually the From URI). If this rule is not required, leave the field empty. To denote any host name, use the asterisk (*) symbol (default).
Destination Username Prefix <b>[IP2IPRouting_DestUsernamePrefix]</b> CLI: dst-user-name-prefix	Defines the prefix of the incoming SIP dialog's destination URI (usually the Request URI) user part. You can use special notations for denoting the prefix. For example, to denote any prefix, use the asterisk (*) symbol; to denote calls without a user part in the URI, use the \$ sign. For available notations, see 'Dialing Plan Notation for Routing and Manipulation' on page 659. The default is * (i.e., any prefix).
Destination Host <b>[IP2IPRouting_DestHost]</b> CLI: dst-host	Defines the host part of the incoming SIP dialog's destination URI (usually the Request-URI). If this rule is not required, leave the field empty. The asterisk (*) symbol (default) can be used to denote any destination host.
Request Type <b>[IP2IPRouting_RequestType]</b> CLI: request-type	Defines the SIP dialog request type of the incoming SIP dialog. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> All (default)</li> <li>▪ <b>[1]</b> INVITE</li> <li>▪ <b>[2]</b> REGISTER</li> <li>▪ <b>[3]</b> SUBSCRIBE</li> <li>▪ <b>[4]</b> INVITE and REGISTER</li> <li>▪ <b>[5]</b> INVITE and SUBSCRIBE</li> <li>▪ <b>[6]</b> OPTIONS</li> </ul>
Message Condition <b>[IP2IPRouting_MessageCondition]</b> CLI: message-condition	Selects a Message Condition rule. To configure Message Condition rules, see 'Configuring Condition Rules' on page 461.
ReRoute IP Group ID <b>[IP2IPRouting_ReRouteIPGroupID]</b> CLI: re-route-ip-group-id	Defines the IP Group that initiated (sent) the SIP redirect response (e.g., 3xx) or REFER message. This field is typically used for re-routing requests (e.g., INVITEs) when interworking is required for SIP 3xx redirect responses or REFER messages (for more information, see 'Interworking SIP 3xx Redirect Responses' on page 436 and 'Interworking SIP REFER Messages' on page 439, respectively). This parameter functions together with the 'Call Trigger' field (see below). The default is -1 (i.e., not configured).
Call Trigger <b>[IP2IPRouting_Trigger]</b> CLI: trigger	Defines the reason (i.e, trigger) for re-routing the SIP request: <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Any = (Default) This routing rule is used for all scenarios (re-routes and non-re-routes).</li> <li>▪ <b>[1]</b> 3xx = Re-routes the request if it was triggered as a result of a SIP 3xx response.</li> <li>▪ <b>[2]</b> REFER = Re-routes the INVITE if it was triggered as a result of a REFER request.</li> <li>▪ <b>[3]</b> 3xx or REFER = Applies to options <b>[1]</b> and <b>[2]</b>.</li> <li>▪ <b>[4]</b> Initial only = This routing rule is used for regular requests that the device forwards to the destination. This rule is not used for re-routing of requests triggered by the receipt of REFER or 3xx.</li> </ul>

Parameter	Description
<b>Operation Routing Rule</b>	
Destination Type <b>[IP2IPRouting_DestType]</b> CLI: dst-type	<p>Determines the destination type to which the outgoing SIP dialog is sent.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> IP Group = (Default) The SIP dialog is sent to the IP Group's Proxy Set (SERVER-type IP Group) or registered contact from the database (if USER-type IP Group).</li> <li>▪ <b>[1]</b> Dest Address = The SIP dialog is sent to the address configured in the following fields: 'Destination SRD ID', 'Destination Address', 'Destination Port', and 'Destination Transport Type'.</li> <li>▪ <b>[2]</b> Request URI = The SIP dialog is sent to the address indicated in the incoming Request-URI. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these fields take precedence.</li> <li>▪ <b>[3]</b> ENUM = An ENUM query is sent to include the destination address. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these fields take precedence.</li> <li>▪ <b>[4]</b> Hunt Group = Used for call center survivability. For more information, see 'Call Survivability for Call Centers' on page 445.</li> <li>▪ <b>[5]</b> Dial Plan = The IP destination is determined by a Dial Plan index of the loaded Dial Plan file. The syntax of the Dial Plan index in the Dial Plan file is as follows: &lt;destination / called prefix number&gt;,0,&lt;IP destination&gt;</li> </ul> <p>Note that the second parameter "0" is ignored. An example of a configured Dial Plan (# 6) in the Dial Plan file is shown below:</p> <pre>[ PLAN6 ] 200,0,10.33.8.52      ; called prefix 200 is routed to destination 10.33.8.52 201,0,10.33.8.52 300,0,itsp.com       ; called prefix 300 is routed to destination itsp.com</pre> <p>Once the Dial Plan is defined, you need to assign it (0 to 7) to the routing rule as the destination in the 'Destination Address' parameter, where "0" denotes <b>[PLAN1]</b>, "1" denotes <b>[PLAN2]</b>, and so on.</p> <ul style="list-style-type: none"> <li>▪ <b>[7]</b> LDAP = LDAP-based routing.</li> </ul>
Destination IP Group ID <b>[IP2IPRouting_DestIPGroupID]</b> CLI: dst-ip-group-id	<p>Defines the IP Group ID to where you want to route the call. The SIP dialog messages are sent to the IP address defined for the Proxy Set associated with this IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Destination Address' field). However, if both parameters are configured, then the IP Group takes precedence.</p> <p>If the destination IP Group is of USER type, the device searches for a match between the Request-URI (of the received SIP dialog) to an AOR registration record in the device's database. The SIP dialog is then sent to the IP address of the registered contact.</p> <p>The default is -1.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is only relevant if the parameter 'Destination Type' is set to 'IP Group'. However, regardless of the settings of the parameter 'Destination Type', the IP Group is still used - only for determining the IP Profile or outgoing SRD. If neither IP Group nor SRD are defined in this table, the destination SRD is determined according to the source SRD associated with the Source IP Group (configured in the IP Group</li> </ul>

Parameter	Description
	<p>table, see 'Configuring IP Groups' on page 204). If this table does not define an IP Group but only an SRD, then the first IP Group associated with this SRD (in the IP Group table) is used.</p> <ul style="list-style-type: none"> <li>▪ If the selected destination IP Group ID is type SERVER, the request is routed according to the IP Group addresses.</li> <li>▪ If the selected destination IP Group ID is type USER, the request is routed according to the IP Group specific database (i.e., only to registered users of the selected database).</li> <li>▪ If the selected destination IP Group ID is ANY USER ([2]), the request is routed according to the general database (i.e., any matching registered user).</li> </ul>
Destination SRD ID <b>[IP2IPRouting_DestSRDID]</b> CLI: dst-srd-id	<p>Defines the SRD ID. The default is None.</p> <p><b>Note:</b> The destination IP Group must belong to the destination SRD if both are configured in this table.</p>
Destination Address <b>[IP2IPRouting_DestAddress]</b> CLI: dst-address	<p>Defines the destination IP address (or domain name, e.g., domain.com) to where the call is sent.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only if the parameter 'Destination Type' is set to 'Dest Address' [1].</li> <li>▪ When using domain names, enter a DNS server IP address or alternatively, define these names in the 'Internal DNS Table' (see 'Configuring the Internal SRV Table' on page 121).</li> </ul>
Destination Port <b>[IP2IPRouting_DestPort]</b> CLI: dst-port	<p>Defines the destination port to where the call is sent.</p>
Destination Transport Type <b>[IP2IPRouting_DestTransportType]</b> CLI: dst-transport-type	<p>Defines the transport layer type for sending the call:</p> <ul style="list-style-type: none"> <li>▪ [-1] Not Configured (default)</li> <li>▪ [0] UDP</li> <li>▪ [1] TCP</li> <li>▪ [2] TLS</li> </ul> <p><b>Note:</b> When this parameter is set to -1, the transport type is determined by the parameter SIPTransportType.</p>
Alternative Route Options <b>[IP2IPRouting_AltRouteOptions]</b> CLI: alt-route-options	<p>Determines whether this routing rule is the main routing rule or an alternative routing rule (to the rule defined directly above it in the table).</p> <ul style="list-style-type: none"> <li>▪ [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.</li> <li>▪ [1] Alt Route Ignore Inputs = If the call cannot be routed to the main route (Route Row), the call is routed to this alternative route regardless of the incoming SIP dialog's input characteristics.</li> <li>▪ [2] Alt Route Consider Inputs = If the call cannot be routed to the main route (Route Row), the call is routed to this alternative route only if the incoming SIP dialog matches this routing rule's input characteristics.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The alternative routing entry ([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.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>For IP-to-IP alternative routing, configure alternative routing reasons upon receipt of 4xx, 5xx, and 6xx SIP responses (see <a href="#">Configuring Alternative Routing Reasons</a> on page 468). However, if no response, ICMP, or a SIP 408 response is received, the device attempts to use the alternative route even if no entries are configured in the 'SBC Alternative Routing Reasons' table.</li> <li>Multiple alternative route entries can be configured (e.g., Index 1 is the main route - Route Row - and indices 2 through 4 are configured as alternative routes).</li> </ul>
Cost Group <b>[IP2IPRouting_CostGroup]</b> CLI: cost-group	Assigns a Cost Group to the routing rule for determining the cost of the call. To configure Cost Groups, see 'Configuring Cost Groups' on page 193.  By default, no Cost Group is assigned to the rule.

### 37.5.4 Blocking Calls from Unregistered SAS Users

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

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

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

### 37.5.5 Configuring SAS Emergency Calls

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

You can define up to four emergency numbers, where each number can include up to four digits. When SAS receives a SIP INVITE (from a UA) that includes one of the user-defined emergency numbers in the SIP user part, it forwards the INVITE directly to the default gateway (see 'SAS Routing in Emergency State' on page 495). The default gateway is defined in the 'SAS Default Gateway IP' field, and this is the device itself. The device then sends the call directly to the PSTN.

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

➤ **To configure SAS emergency numbers:**

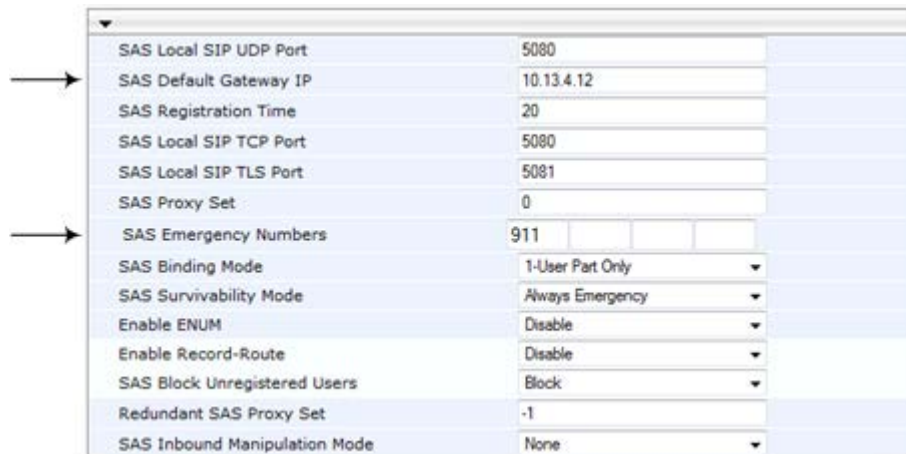
1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. In the 'SAS Default Gateway IP' field, define the IP address and port (in the format x.x.x.x:port) of the device (Gateway application).



**Note:** The port of the device is defined in the 'SIP UDP/TCP/TLS Local Port' field in the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

3. In the 'SAS Emergency Numbers' field, enter an emergency number in each field box.

**Figure 37-10: Configuring SAS Emergency Numbers**



SAS Local SIP UDP Port	5080
SAS Default Gateway IP	10.13.4.12
SAS Registration Time	20
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	0
SAS Emergency Numbers	911
SAS Binding Mode	1-User Part Only
SAS Survivability Mode	Always Emergency
Enable ENUM	Disable
Enable Record-Route	Disable
SAS Block Unregistered Users	Block
Redundant SAS Proxy Set	-1
SAS Inbound Manipulation Mode	None

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

### 37.5.6 Adding SIP Record-Route Header to SIP INVITE

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

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



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

#### ➤ To enable the Record-Route header:

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

### 37.5.7 Re-using TCP Connections

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

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

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

### 37.5.8 Replacing Contact Header for SIP Messages

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



**Notes:**

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

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

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

## 37.6 Viewing Registered SAS Users

You can view all the users that are registered in the SAS registration database. This is displayed in the 'SAS/SBC Registered Users' page, as described in 'Viewing Registered Users' on page [594](#).



**Note:** You can increase the maximum number of registered SAS users, by implementing the SAS Cascading feature, as described in 'SAS Cascading' on page [517](#).



## 38 SAS Cascading

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

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

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

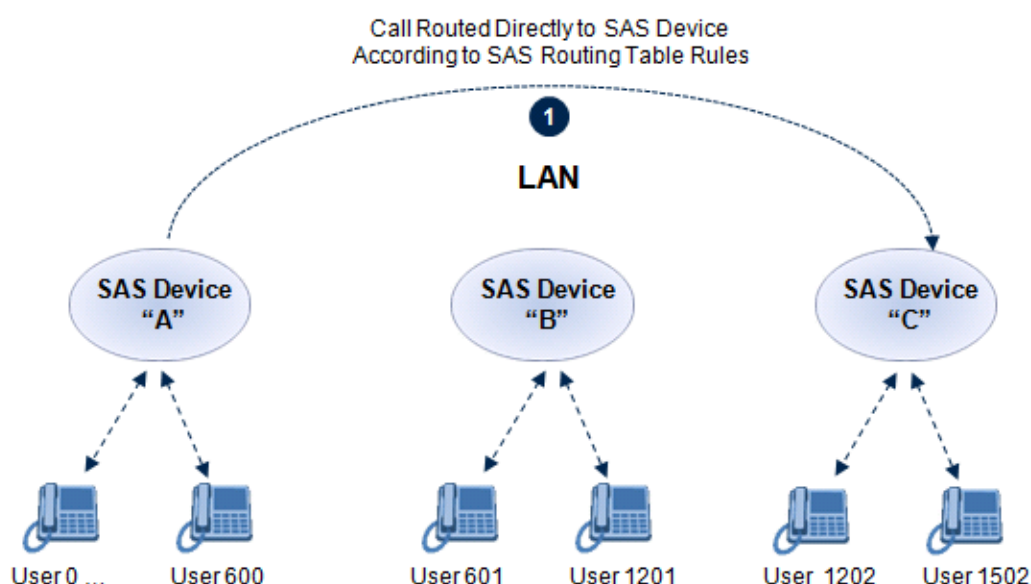
- **SAS Routing Table:** If users can be identified with unique phone extension numbers, then the SAS Routing table is used to configure SAS Cascading. This SAS Cascading method routes calls directly to the SAS Gateway (defined by IP address) to which the called SAS user is registered.

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

- users registered to the first SAS gateway start with extension number "40"
- users registered to the second SAS gateway start with extension number "20"
- users registered to the third SAS gateway start with extension number "30"

The SAS Routing table rules for SAS Cascading are created using the destination (called) extension number prefix (e.g., "30") and the destination IP address of the SAS gateway to which the called user is registered. Such SAS routing rules must be configured at each SAS gateway to allow routing between the SAS users. The routing logic for SAS Cascading is similar to SAS routing in Emergency state (see the flowchart in 'SAS Routing in Emergency State' on page 495). For a description on the SAS Routing table, see 'SAS Routing Based on IP-to-IP Routing Table' on page 508.

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



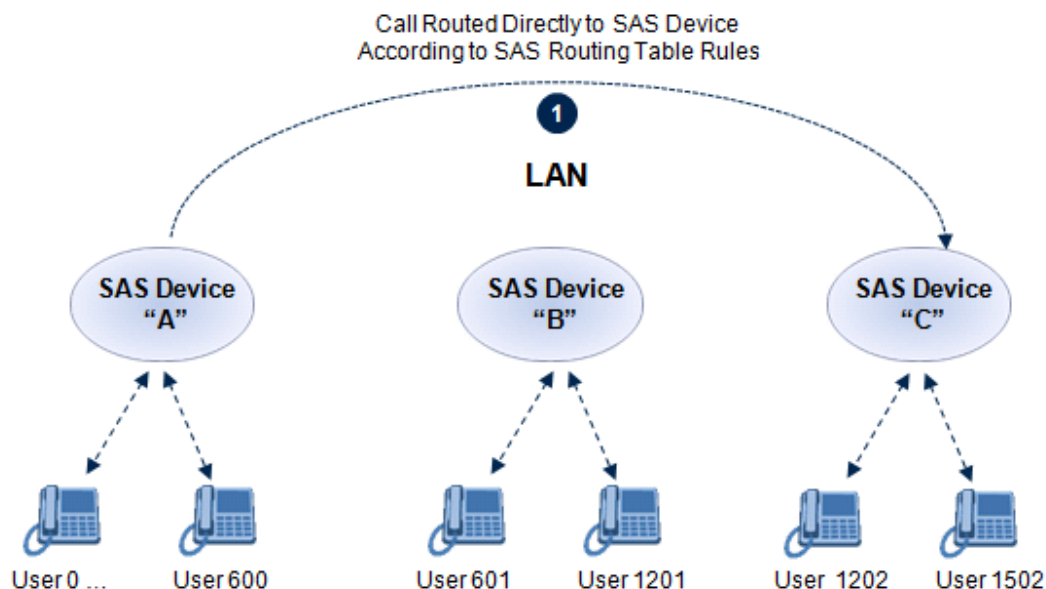
**Figure 38-1: SAS Cascading Using SAS Routing Table - Example**

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

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

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

**Figure 38-2: SAS Cascading Using SAS Redundancy Mode - Example**



# Part IX

## IP Media Capabilities



## 39 Transcoding using Third-Party Call Control

The device supports transcoding using a third-party call control Application server. This support is provided by the following:

- Using RFC 4117 (see 'Using RFC 4117' on page 521)



**Note:** Transcoding can also be implemented using the IP-to-IP application and SBC application.

### 39.1 Using RFC 4117

The device supports RFC 4117 - Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc) - providing transcoding services (i.e., acting as a transcoding server). This is used in scenarios where two SIP User Agents (UA) would like to establish a session, but do not have a common coder or media type. When such incompatibilities are found, the UAs need to invoke transcoding services to successfully establish the session. Note that transcoding can also be performed using NetAnn, according to RFC 4240.

To enable the RFC 4117 feature, the parameter EnableRFC4117Transcoding must be set to 1 (and the device must be reset).

The 3pcc call flow is as follows: The device receives from one of the UAs, a single INVITE with an SDP containing two media lines. Each media represents the capabilities of each of the two UAs. The device needs to find a match for both of the media, and opens two channels with two different media ports to the different UAs. The device performs transcoding between the two voice calls.

In the example below, an Application Server sends a special INVITE that consists of two media lines to perform transcoding between G.711 and G.729:

```
m=audio 20000 RTP/AVP 0
c=IN IP4 A.example.com
m=audio 40000 RTP/AVP 18
c=IN IP4 B.example.com
```

## Reader's Notes

# Part X

## Data-Router Configuration





## 40 Introduction



**Note:** To configure the device's Data-Router functionality, use the CLI. For more information, refer to the document, *MSBR Series CLI Reference Guide for Data Functionality*.

## Reader's Notes

# Part XI

## Maintenance



## 41 Basic Maintenance

The Maintenance Actions page allows you to perform the following:

- Reset the device - see 'Resetting the Device' on page 529
- Lock and unlock the device - see 'Locking and Unlocking the Device' on page 531
- Save configuration to the device's flash memory - see 'Saving Configuration' on page 532

➤ To access the Maintenance Actions page, do one of the following:

- On the toolbar, click the **Device Actions** button, and then from the drop-down menu, choose **Reset**.
- On the Navigation bar, click the **Maintenance** tab, and then in the Navigation tree, select the **Maintenance** menu and choose **Maintenance Actions**.

**Figure 41-1: Maintenance Actions Page**

▼ Reset Configuration	
Reset Board	<input type="button" value="Reset"/>
Burn To FLASH	Yes <input type="button" value="v"/>
Graceful Option	No <input type="button" value="v"/>
▼ LOCK / UNLOCK	
Lock	<input type="button" value="LOCK"/>
Graceful Option	No <input type="button" value="v"/>
Current Admin State	UNLOCKED
▼ Save Configuration	
Burn To FLASH	<input type="button" value="BURN"/>

### 41.1 Resetting the Device

The Maintenance Actions page allows you to remotely reset the device. In addition, before resetting the device, you can choose the following options:

- Save the device's current configuration to the device's flash memory (non-volatile).
- Perform a graceful shutdown, whereby device reset starts only after a user-defined time (i.e., timeout) or after no more active traffic exists (the earliest thereof).



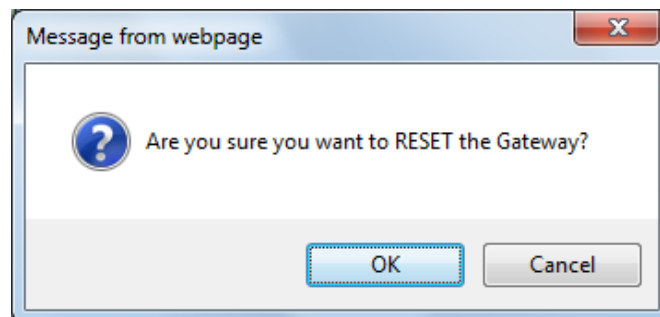
**Notes:**

- Throughout the Web interface, parameters displayed with a lightning ⚡ symbol are not applied on-the-fly and require that you reset the device for them to take effect.
- When you modify parameters that require a device reset, once you click the **Submit** button in the relevant page, the toolbar displays "Reset" (see 'Toolbar Description' on page 41) to indicate that a device reset is required.
- After you reset the device, the Web GUI is displayed in Basic view (see 'Displaying Navigation Tree in Basic and Full View' on page 43).
- Upon reboot, the device restores the settings from its configuration file. However, if reboot attempts fail three times consecutively, the device resets the configuration file by restoring factory defaults before attempting to reboot.

➤ **To reset the device:**

1. Open the Maintenance Actions page (see 'Basic Maintenance' on page 529).
2. Under the 'Reset Configuration' group, from the 'Burn To FLASH' drop-down list, select one of the following options:
  - **Yes:** The device's current configuration is saved (*burned*) to the flash memory prior to reset (default).
  - **No:** Resets the device without saving the current configuration to flash (discards all unsaved modifications).
3. Under the 'Reset Configuration' group, from the 'Graceful Option' drop-down list, select one of the following options:
  - **Yes:** Reset starts only after the user-defined time in the 'Shutdown Timeout' field (see Step 4) expires or after no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
  - **No:** Reset starts regardless of traffic, and any existing traffic is terminated at once.
4. In the 'Shutdown Timeout' field (relevant only if the 'Graceful Option' in the previous step is set to **Yes**), enter the time after which the device resets. Note that if no traffic exists and the time has not yet expired, the device resets.
5. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.

**Figure 41-2: Reset Confirmation Message Box**



6. Click **OK** to confirm device reset; if the parameter 'Graceful Option' is set to **Yes** (in Step 3), the reset is delayed and a screen displaying the number of remaining calls and time is displayed. When the device begins to reset, a message appears notifying you of this.

## 41.2 Remotely Resetting Device using SIP NOTIFY

The device can be remotely reset upon the receipt of a SIP NOTIFY that includes an Event header set to 'check-sync;reboot=true', as shown in the example below:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
From: sip:sipsak@<srchost>
CSeq: 10 NOTIFY
Call-ID: 1234@<srchost>
Event: check-sync;reboot=true
```

➤ **To enable remote reset upon receipt of SIP NOTIFY:**

1. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).
2. Under the Misc Parameters group, set the 'SIP Remote Rest' parameter to **Enable**.
3. Click **Submit**.



**Note:** This SIP Event header value is proprietary to AudioCodes.

## 41.3 Locking and Unlocking the Device

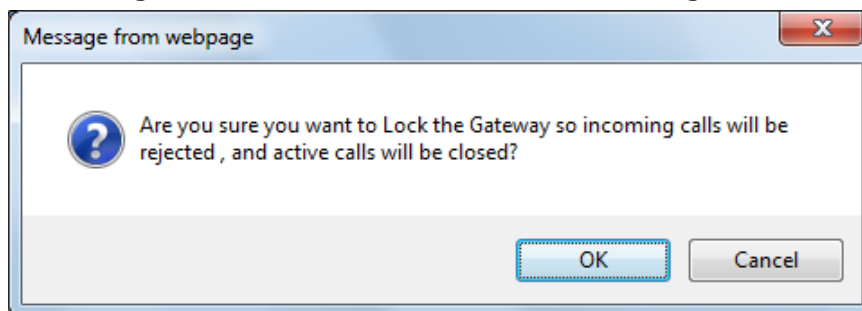
The Lock and Unlock option allows you to lock the device so that it doesn't accept any new calls and maintains only the current calls. This is useful when, for example, you are uploading new software files to the device and you don't want any traffic to interfere with the process.

➤ **To lock the device:**

1. Open the Maintenance Actions page (see 'Basic Maintenance' on page 529).
2. Under the 'LOCK / UNLOCK' group, from the 'Graceful Option' drop-down list, select one of the following options:
  - **Yes:** The device is 'locked' only after the user-defined time in the 'Lock Timeout' field (see Step 3) expires or no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
  - **No:** The device is 'locked' regardless of traffic. Any existing traffic is terminated immediately.

**Note:** These options are only available if the current status of the device is in the Unlock state.
3. In the 'Lock Timeout' field (relevant only if the parameter 'Graceful Option' in the previous step is set to **Yes**), enter the time (in seconds) after which the device locks. Note that if no traffic exists and the time has not yet expired, the device locks.
4. Click the **LOCK** button; a confirmation message box appears requesting you to confirm device Lock.

**Figure 41-3: Device Lock Confirmation Message Box**



5. Click **OK** to confirm device Lock; if 'Graceful Option' is set to **Yes**, the lock is delayed and a screen displaying the number of remaining calls and time is displayed. Otherwise, the lock process begins immediately. The Current Admin State' field displays the current state - "LOCKED" or "UNLOCKED".

➤ **To unlock the device:**

1. Open the Maintenance Actions page (see 'Maintenance Actions' on page 529).
2. Under the 'LOCK / UNLOCK' group, click the **UNLOCK** button. Unlock starts immediately and the device accepts new incoming calls.



**Note:** The Home page's General Information pane displays whether the device is locked or unlocked (see 'Viewing the Home Page' on page 54).

## 41.4 Saving Configuration

The Maintenance Actions page allows you to save (*burn*) the current parameter configuration (including loaded auxiliary files) to the device's *non-volatile* memory (i.e., flash). The parameter modifications that you make throughout the Web interface's pages are temporarily saved (to the *volatile* memory - RAM) when you click the **Submit** button on these pages. Parameter settings that are saved only to the device's RAM revert to their previous settings after a hardware/software reset (or power failure). Therefore, to ensure that your configuration changes are retained, you must save them to the device's flash memory using the burn option described below.

➤ **To save the changes to the non-volatile flash memory :**

1. Open the Maintenance Actions page (see 'Basic Maintenance' on page 529).
2. Under the 'Save Configuration' group, click the **BURN** button; a confirmation message appears when the configuration successfully saves.



**Notes:**

- Saving configuration to the *non-volatile* memory may disrupt current traffic on the device. To avoid this, disable all new traffic before saving, by performing a graceful lock (see 'Locking and Unlocking the Device' on page 531).
- Throughout the Web interface, parameters displayed with the lightning ⚡ symbol are not applied on-the-fly and require that you reset the device for them to take effect (see 'Resetting the Device' on page 529).
- The Home page's General Information pane displays whether the device is currently "burning" the configuration (see 'Viewing the Home Page' on page 54).



## 42 Resetting Channels

### 42.1 Resetting an Analog Channel

You can inactivate (*reset*) an FXO or FXS analog channel. This is sometimes useful, for example, when the device (FXO) is connected to a PBX and the communication between the two can't be disconnected (e.g., when using reverse polarity). This is done in the Web interface's Home page.

➤ **To reset an analog channel:**

1. Open the Home page.
2. Click the required **FXS** or **FXO** port icon; a shortcut menu appears.
3. From the shortcut menu, choose **Reset Channel**; the channel is changed to inactive and the port icon is displayed in gray.

### 42.2 Restarting a B-Channel

You can restart a specific B-channel belonging to an ISDN or CAS trunk, using the SNMP MIB variable, `acTrunkISDNCommonRestartBChannel` or the EMS management tool (refer to the EMS User's Manual). This may be useful, for example, for troubleshooting specific voice channels.



**Notes:**

- If a voice call is currently in progress on the B-channel, it is disconnected when the B-channel is restarted.
- B-channel restart can only be done if the D-channel of the trunk to which it belongs is synchronized (Layer 2).
- B-channel restart does not affect the B-channel's configuration.

## Reader's Notes

## 43 Software Upgrade

The **Software Update** menu allows you to do the following:

- Load Auxiliary files (see 'Loading Auxiliary Files' on page 535)
- Load a Software License Key (see 'Software License Key' on page 552)
- Upgrade the device using the Software Upgrade Wizard (see 'Software Upgrade Wizard' on page 555)
- Load/save a Configuration file (see 'Backing Up and Loading Configuration File' on page 558)

### 43.1 Loading Auxiliary Files

Various Auxiliary files can be installed on the device. These Auxiliary files provide the device with additional configuration settings. The table below lists the different types of Auxiliary files:

**Auxiliary Files**

File	Description
INI	Configures the device. The Web interface enables practically full device provisioning. However, some features may only be configured by ini file or you may wish to configure your device using the ini file. For more information on using the ini file to configure the device, see 'INI File-Based Management' on page 89.
CAS	CAS auxiliary files containing the CAS Protocol definitions for CAS-terminated trunks (for various types of CAS signaling). You can use the supplied files or construct your own files. Up to eight different CAS files can be installed on the device. For more information, see CAS Files on page 541.
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 537.
Dial Plan	Provides dialing plans, for example, to know when to stop collecting dialed digits and start forwarding them or for obtaining the destination IP address for outbound IP routing. For more information, see 'Dial Plan File' on page 541.
User Info	The User Information file maps PBX extensions to IP numbers. This file can be used to represent PBX extensions as IP phones in the global 'IP world'. For more information, see 'User Information File' on page 547.

The Auxiliary files can be loaded to the device using one of the following methods:

- Web interface.
- TFTP: This is done by specifying the name of the Auxiliary file in an *ini* file (see Auxiliary and Configuration Files Parameters) and then loading the *ini* file to the device. The Auxiliary files listed in the *ini* file are then automatically loaded through TFTP during device startup. If the *ini* file does not contain a specific auxiliary file type, the device uses the last auxiliary file of that type that was stored on its non-volatile memory.

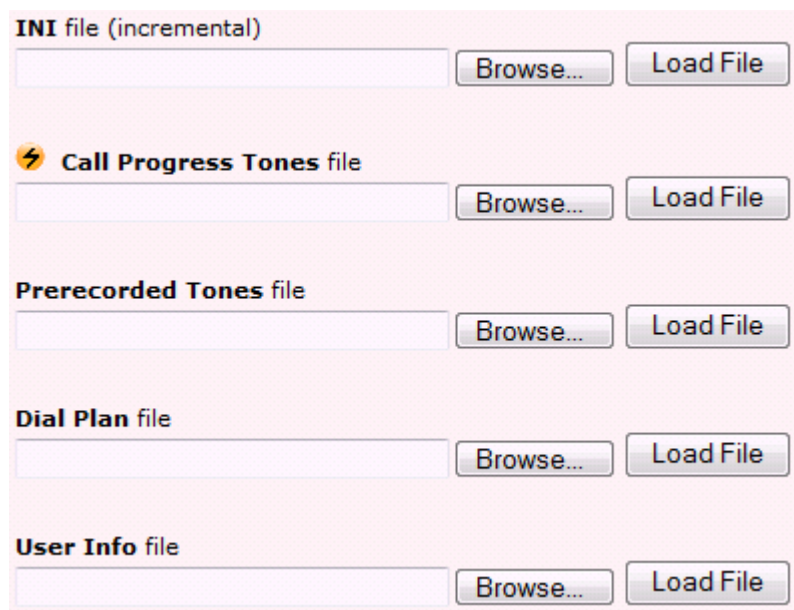

**Notes:**

- You can schedule automatic loading of updated auxiliary files using HTTP/HTTPS. For more information on automatic updates, see 'Automatic Update' on page 561.
- When loading an *ini* file using this Web page, parameters that are excluded from the loaded *ini* file retain their current settings (*incremental*).
- Saving an auxiliary file to flash memory may disrupt traffic on the device. To avoid this, disable all traffic on the device by performing a graceful lock as described in 'Locking and Unlocking the Device' on page 531.
- For deleting auxiliary files, see 'Viewing Device Information' on page 577.

The procedure below describes how to load Auxiliary files using the Web interface.

➤ **To load auxiliary files to the device using the Web interface:**

1. Open the Load Auxiliary Files page (**Maintenance** tab > **Software Update** menu > **Load Auxiliary Files**).




**Note:** The appearance of certain file load fields depends on the installed Software License Key.

2. Click the **Browse** button corresponding to the file type that you want to load, navigate to the folder in which the file is located, and then click **Open**; the name and path of the file appear in the field next to the **Browse** button.
3. Click the **Load File** button corresponding to the file you want to load.
4. Repeat steps 2 through 3 for each file you want to load.
5. Save the loaded auxiliary files to flash memory, see 'Saving Configuration' on page 532 and reset the device (if you have loaded a Call Progress Tones file), see 'Resetting the Device' on page 529.

### 43.1.1 Call Progress Tones File

The Call Progress Tones (CPT) and Distinctive Ringing (applicable to analog interfaces) auxiliary file is comprised of two sections:

- The first section contains the definitions of the Call Progress Tones (levels and frequencies) that are detected/generated by the device.
- The second section contains the characteristics of the Distinctive Ringing signals that are generated by the device (see Distinctive Ringing on page 539).

You can use one of the supplied auxiliary files (.dat file format) or create your own file. To create your own file, it's recommended to modify the supplied *usa\_tone.ini* file (in any standard text editor) to suit your specific requirements and then convert the modified *ini* file into binary format, using AudioCodes DConvert utility. For a description on converting a CPT *ini* file into a binary *dat* file, refer to the *DConvert Utility User's Guide*.



**Note:** Only the *dat* file format can be loaded to the device.

You can create up to 32 different Call Progress Tones, each with frequency and format attributes. The frequency attribute can be single or dual-frequency (in the range of 300 to 1980 Hz) or an Amplitude Modulated (AM). Up to 64 different frequencies are supported. Only eight AM tones, in the range of 1 to 128 kHz, can be configured (the detection range is limited to 1 to 50 kHz). Note that when a tone is composed of a single frequency, the second frequency field must be set to zero.

The format attribute can be one of the following:

- **Continuous:** A steady non-interrupted sound (e.g., a dial tone). Only the 'First Signal On time' should be specified. All other on and off periods must be set to zero. In this case, the parameter specifies the detection period. For example, if it equals 300, the tone is detected after 3 seconds (300 x 10 msec). The minimum detection time is 100 msec.
- **Cadence:** A repeating sequence of on and off sounds. Up to four different sets of on/off periods can be specified.
- **Burst:** A single sound followed by silence. Only the 'First Signal On time' and 'First Signal Off time' should be specified. All other on and off periods must be set to zero. The burst tone is detected after the off time is completed.

You can specify several tones of the same type. These additional tones are used only for tone detection. Generation of a specific tone conforms to the first definition of the specific tone. For example, you can define an additional dial tone by appending the second dial tone's definition lines to the first tone definition in the *ini* file. The device reports dial tone detection if either of the two tones is detected.

The Call Progress Tones section of the *ini* file comprises the following segments:

- **[NUMBER OF CALL PROGRESS TONES]:** Contains the following key:  
'Number of Call Progress Tones' defining the number of Call Progress Tones that are defined in the file.
- **[CALL PROGRESS TONE #X]:** containing the Xth tone definition, starting from 0 and not exceeding the number of Call Progress Tones less 1 defined in the first section (e.g., if 10 tones, then it is 0 to 9), using the following keys:
  - **Tone Type:** Call Progress Tone types:
    - ◆ **[1]** Dial Tone
    - ◆ **[2]** Ringback Tone

- ◆ [3] Busy Tone
- ◆ [4] Congestion Tone
- ◆ [6] Warning Tone
- ◆ [7] Reorder Tone
- ◆ [8] Confirmation Tone
- ◆ [9] Call Waiting Tone - heard by the called party
- ◆ [15] Stutter Dial Tone
- ◆ [16] Off Hook Warning Tone
- ◆ [17] Call Waiting Ringback Tone - heard by the calling party
- ◆ [18] Comfort Tone
- ◆ [23] Hold Tone
- ◆ [46] Beep Tone
- **Tone Modulation Type:** Amplitude Modulated (1) or regular (0)
- **Tone Form:** The tone's format can be one of the following:
  - ◆ Continuous (1)
  - ◆ Cadence (2)
  - ◆ Burst (3)
- **Low Freq [Hz]:** Frequency (in Hz) of the lower tone component in case of dual frequency tone, or the frequency of the tone in case of single tone. This is not relevant to AM tones.
- **High Freq [Hz]:** Frequency (in Hz) of the higher tone component in case of dual frequency tone, or zero (0) in case of single tone (not relevant to AM tones).
- **Low Freq Level [-dBm]:** Generation level 0 dBm to -31 dBm in dBm (not relevant to AM tones).
- **High Freq Level:** Generation level of 0 to -31 dBm. The value should be set to 32 in the case of a single tone (not relevant to AM tones).
- **First Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the first cadence on-off cycle. For continuous tones, this parameter defines the detection period. For burst tones, it defines the tone's duration.
- **First Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the first cadence on-off cycle (for cadence tones). For burst tones, this parameter defines the off time required after the burst tone ends and the tone detection is reported. For continuous tones, this parameter is ignored.
- **Second Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the second cadence on-off cycle. Can be omitted if there isn't a second cadence.
- **Second Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the second cadence on-off cycle. Can be omitted if there isn't a second cadence.
- **Third Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the third cadence on-off cycle. Can be omitted if there isn't a third cadence.
- **Third Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the third cadence on-off cycle. Can be omitted if there isn't a third cadence.
- **Fourth Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the fourth cadence on-off cycle. Can be omitted if there isn't a fourth cadence.
- **Fourth Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the fourth cadence on-off cycle. Can be omitted if there isn't a fourth cadence.
- **Carrier Freq [Hz]:** Frequency of the carrier signal for AM tones.
- **Modulation Freq [Hz]:** Frequency of the modulated signal for AM tones (valid range from 1 to 128 Hz).

- **Signal Level [-dBm]:** Level of the tone for AM tones.
- **AM Factor [steps of 0.02]:** Amplitude modulation factor (valid range from 1 to 50). Recommended values from 10 to 25.



**Notes:**

- When the same frequency is used for a continuous tone and a cadence tone, the 'Signal On Time' parameter of the continuous tone must have a value that is greater than the 'Signal On Time' parameter of the cadence tone. Otherwise, the continuous tone is detected instead of the cadence tone.
- The tones frequency must differ by at least 40 Hz between defined tones.

For example, to configure the dial tone to 440 Hz only, enter the following text:

```
[NUMBER OF CALL PROGRESS TONES]
Number of Call Progress Tones=1
#Dial Tone
[CALL PROGRESS TONE #0]
Tone Type=1
Tone Form =1 (continuous)
Low Freq [Hz]=440
High Freq [Hz]=0
Low Freq Level [-dBm]=10 (-10 dBm)
High Freq Level [-dBm]=32 (use 32 only if a single tone is
required)
First Signal On Time [10msec]=300; the dial tone is detected after
3 sec
First Signal Off Time [10msec]=0
Second Signal On Time [10msec]=0
Second Signal Off Time [10msec]=0
```

#### 43.1.1.1 Distinctive Ringing

Distinctive Ringing is applicable only to FXS interfaces. Using the Distinctive Ringing section of the Call Progress Tones auxiliary file, you can create up to 16 Distinctive Ringing patterns. Each ringing pattern configures the ringing tone frequency and up to four ringing cadences. The same ringing frequency is used for all the ringing pattern cadences. The ringing frequency can be configured in the range of 10 to 200 Hz with a 5 Hz resolution.

Each of the ringing pattern cadences is specified by the following parameters:

- **Burst Ring On Time:** Configures the cadence to be a burst cadence in the entire ringing pattern. The burst relates to On time and the Off time of the same cadence. It must appear between 'First/Second/Third/Fourth' string and the 'Ring On/Off Time'. This cadence rings once during the ringing pattern. Otherwise, the cadence is interpreted as cyclic: it repeats for every ringing cycle.
- **Ring On Time:** Specifies the duration of the ringing signal.
- **Ring Off Time:** Specifies the silence period of the cadence.

The Distinctive Ringing section of the *ini* file format contains the following strings:

- **[NUMBER OF DISTINCTIVE RINGING PATTERNS]:** Contains the following key:
  - 'Number of Distinctive Ringing Patterns' defining the number of Distinctive Ringing signals that are defined in the file.

- **[Ringing Pattern #X]:** Contains the Xth ringing pattern definition (starting from 0 and not exceeding the number of Distinctive Ringing patterns defined in the first section minus 1) using the following keys:
  - **Ring Type:** Must be equal to the Ringing Pattern number.
  - **Freq [Hz]:** Frequency in hertz of the ringing tone.
  - **First (Burst) Ring On Time [10 msec]:** 'Ring On' period (in 10 msec units) for the first cadence on-off cycle.
  - **First (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the first cadence on-off cycle.
  - **Second (Burst) Ring On Time [10 msec]:** 'Ring On' period (in 10 msec units) for the second cadence on-off cycle.
  - **Second (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the second cadence on-off cycle.
  - **Third (Burst) Ring On Time [10 msec]:** 'Ring On' period (in 10 msec units) for the third cadence on-off cycle.
  - **Third (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the third cadence on-off cycle.
  - **Fourth (Burst) Ring On Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the fourth cadence on-off cycle.
  - **Fourth (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the fourth cadence on-off cycle.



**Note:** In SIP, the Distinctive Ringing pattern is selected according to the Alert-Info header in the INVITE message. For example:  
 Alert-Info:<Bellcore-dr2>, or Alert-Info:<http://.../Bellcore-dr2>  
 'dr2' defines ringing pattern #2. If the Alert-Info header is missing, the default ringing tone (0) is played.

An example of a **ringing burst** definition is shown below:

```
#Three ringing bursts followed by repeated ringing of 1 sec on and
3 sec off.
[NUMBER OF DISTINCTIVE RINGING PATTERNS]
Number of Ringing Patterns=1
[Ringing Pattern #0]
Ring Type=0
Freq [Hz]=25
First Burst Ring On Time [10msec]=30
First Burst Ring Off Time [10msec]=30
Second Burst Ring On Time [10msec]=30
Second Burst Ring Off Time [10msec]=30
Third Burst Ring On Time [10msec]=30
Third Burst Ring Off Time [10msec]=30
Fourth Ring On Time [10msec]=100
Fourth Ring Off Time [10msec]=300
```

An example of **various ringing signals** definition is shown below:

```
[NUMBER OF DISTINCTIVE RINGING PATTERNS]
Number of Ringing Patterns=3
#Regular North American Ringing Pattern
[Ringing Pattern #0]
Ring Type=0
Freq [Hz]=20
First Ring On Time [10msec]=200
First Ring Off Time [10msec]=400
```



```
#GR-506-CORE Ringing Pattern 1
[Ringing Pattern #1]
Ring Type=1
Freq [Hz]=20
First Ring On Time [10msec]=200
First Ring Off Time [10msec]=400
#GR-506-CORE Ringing Pattern 2
[Ringing Pattern #2]
Ring Type=2
Freq [Hz]=20
First Ring On Time [10msec]=80
First Ring Off Time [10msec]=40
Second Ring On Time [10msec]=80
Second Ring Off Time [10msec]=400
```

### 43.1.2 CAS Files

The CAS auxiliary files contain the CAS Protocol definitions that are used for CAS-terminated trunks. You can use the supplied files or construct your own files. Up to eight files can be loaded to the device. Different files can be assigned to different trunks (CASTableIndex\_x) and different CAS tables can be assigned to different B-channels (CASChannelIndex).

The CAS files can be loaded to the device using the Web interface or *ini* file (see 'Loading Auxiliary Files' on page 535).



**Note:** All CAS files loaded together must belong to the same Trunk Type (i.e., either E1 or T1).

### 43.1.3 Dial Plan File

The Dial Plan file can be used for various digit mapping features, as described in this section.

#### 43.1.3.1 Creating a Dial Plan File

Creating a Dial Plan file is similar between all Dial Plan features. The main difference is the syntax used in the Dial Plan file and the method for selecting the Dial Plan index to use for the specific feature.

The Dial Plan file is a text-based file that can contain up to eight Dial Plans (Dial Plan indices) and up to 8,000 rules (lines). The general syntax rules for the Dial Plan file are as follows (syntax specific to the feature is described in the respective section):

- Each Dial Plan index must begin with a Dial Plan name enclosed in square brackets "[...]" on a new line.
- Each line under the Dial Plan index defines a rule.
- Empty lines are ignored.
- Lines beginning with a semicolon ";" are ignored. The semicolon can be used for comments.

➤ **To create a Dial Plan file:**

1. Create a new file using a text-based editor (such as Notepad) and configure your Dial Plans, as required.
2. Save the file with the *ini* file extension name (e.g., mydialplanfile.ini).
3. Convert the *ini* file to a *dat* binary file, using AudioCodes DConvert utility. For more information, refer to *DConvert Utility User's Guide*.
4. Install the converted file on the device, as described in 'Loading Auxiliary Files' on page 535.
5. Select the Dial Plan index that you want to use. This depends on the feature and is described in the respective section.

### 43.1.3.2 Dialing Plans for Digit Collection

The device enables you to configure multiple dialing plans in an external Dial Plan file, which can be installed on the device. If a Dial Plan file is implemented, the device first attempts to locate a matching digit pattern in a specified Dial Plan index listed in the file and if not found, attempts to locate a matching digit pattern in the Digit Map. The Digit Map is configured by the 'Digit Mapping Rules' parameter, located in the DTMF & Dialing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **DTMF and Supplementary** > **DTMF & Dialing**).

The Dial Plan is used for the following:

- ISDN Overlap Dialing, FXS, and FXO collecting digit mode (Tel-to-IP calls): The file allows the device to know when digit collection ends, after which it starts sending all the collected (or dialed) digits in the outgoing INVITE message. This also provides enhanced digit mapping.
- CAS E1 MF-CR2 (Tel-to-IP calls): Useful for E1 MF-CR2 variants that do not support I-15 terminating digits (e.g., in Brazil and Mexico). The Dial Plan file allows the device to detect end-of-dialing in such cases. The CasTrunkDialPlanName\_x ini file parameter determines which dial plan (in the Dial Plan file) to use for a specific trunk.



**Notes:**

- To use the Dial Plan file, you must also use a special CAS .dat file that supports this feature. For more information, contact your AudioCodes sales representative.
- For E1 CAS MFC-R2 variants, which don't support terminating digit for the called party number, usually I-15, the Dial Plan file and the DigitMapping parameter are ignored. Instead, you can define a Dial Plan template per trunk using the parameter CasTrunkDialPlanName\_x.

The Dial Plan file can contain up to eight Dial Plans (Dial Plan indices), with a total of up to 8,000 dialing rules (lines) of distinct prefixes (e.g. area codes, international telephone number patterns) for the PSTN to which the device is connected.

The Dial Plan file is created in a textual *ini* file with the following syntax:

```
<called number prefix>,<total digits to wait before sending>
```

- Each new Dial Plan index begins with a Dial Plan name enclosed in square brackets "[...]" on a new line.
- Each line under the Dial Plan index defines a dialing prefix and the number of digits expected to follow that prefix. The prefix is separated by a comma "," from the number of additional digits.
- The prefix can include numerical ranges in the format [x-y], as well as multiple numerical ranges [n-m][x-y] (no comma between them).

- The prefix can include the asterisk "\*" and number "#" signs.
- The number of additional digits can include a numerical range in the format x-y.
- Empty lines are ignored.
- Lines beginning with a semicolon ";" are ignored. The semicolon can be used for comments.

Below shows an example of a Dial Plan file (in *ini*-file format), containing two dial plans:

```
; Example of dial-plan configuration.
; This file contains two dial plans:
[ PLAN1 ]
; Destination cellular area codes 052, 054, and 050 with 8 digits.

052,8
054,8
050,8
; Defines International prefixes 00, 012, 014.
; The number following these prefixes may
; be 7 to 14 digits in length.
00,7-14
012,7-14
014,7-14
; Defines emergency number 911. No additional digits are expected.
911,0
[ PLAN2 ]
; Defines area codes 02, 03, 04.
; In these area codes, phone numbers have 7 digits.
0[2-4],7
; Operator services starting with a star: *41, *42, *43.
; No additional digits are expected.
*4[1-3],0
```

The procedure below provides a summary on how to create a Dial Plan file and select the required 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., mydialplans.ini).
3. Convert the *ini* file to a *dat* binary file, using AudioCodes DConvert utility. For more information, refer to *DConvert Utility User's Guide*.
4. Install the converted file on the device, as described in 'Loading Auxiliary Files' on page 535.
5. The required Dial Plan is selected using the 'Dial Plan Index' parameter. This parameter can be set to 0 through 7, where 0 denotes PLAN1, 1 denotes PLAN2, and so on.


**Notes:**

- The Dial Plan file must not contain overlapping prefixes. Attempting to process an overlapping configuration by the DConvert utility results in an error message specifying the problematic line.
- The Dial Plan index can be selected globally for all calls (as described in the previous procedure), or per specific calls using Tel Profiles.
- It may be useful to configure both Dial Plan file and Digit Maps. For example, the Digit Map can be used for complex digit patterns (which are not supported by the Dial Plan) and the Dial Plan can be used for long lists of relatively simple digit patterns. In addition, as timeout between digits is not supported by the Dial Plan, the Digit Map can be used to configure digit patterns that are shorter than those defined in the Dial Plan or left at default (MaxDigits parameter). For example, the "xx.T" digit map instructs the device to use the Dial Plan and if no matching digit pattern is found, it waits for two more digits and then after a timeout (TimeBetweenDigits parameter), it sends the collected digits. Therefore, this ensures that calls are not rejected as a result of their digit pattern not been completed in the Dial Plan.
- By default, if no matching digit pattern is found in both the Dial Plan and Digit Map, the device rejects the call. However, if you set the DisableStrictDialPlan parameter to 1, the device attempts to complete the call using the MaxDigits and TimeBetweenDigits parameters. In such a setup, it collects the number of digits configured by the MaxDigits parameters. If more digits are received, it ignores the settings of this parameter and collects the digits until the inter-digit timeout configured by the TimeBetweenDigits parameter is exceeded.

### 43.1.3.3 Dial Plan Prefix Tags for IP-to-Tel Routing

The device supports the use of string labels (or "tags") in the external Dial Plan file for tagging incoming IP-to-Tel calls. The special "tag" is added as a prefix to the called party number, and then the Inbound IP Routing Table uses this "tag" instead of the original prefix. Manipulation is then performed after routing in the Manipulation table, which strips the "tag" characters before sending the call to the endpoint.

This feature resolves the limitation of entries in the Inbound IP Routing Table (IP-to-Tel call routing) for scenarios in which many different routing rules are required. For example, a city may have many different area codes, some for local calls and others for long distance calls (e.g. 425-202-xxxx for local calls, but 425-200-xxxx for long distance calls).

For using tags, the Dial Plan file is defined as follows:

- Number of dial plan (text)
- Dial string prefix (ranges can be defined in brackets)
- User-defined routing tag (text)



**Note:** Dial Plan Prefix Tags are not applicable to FXS and FXO interfaces.

The example configuration below assumes a scenario where multiple prefixes exist for local and long distance calls:

➤ **To use Dial Plan file routing tags:**

1. Load an *ini* file to the device that selects Dial Plan index (e.g., 1) for routing tags, as shown below:

```
IP2TelTaggingDestDialPlanIndex = 0
```

2. Define the external Dial Plan file with two routing tags (as shown below):

- "LOCL" - for local calls
- "LONG" - for long distance calls

```
[ PLAN1 ]
42520[3-5],0,LOCL
425207,0,LOCL
42529,0,LOCL
425200,0,LONG
425100,0,LONG
```

For example, if an incoming IP call to destination prefix 425203 is received, the device adds the prefix tag "LOCL" as specified in the Dial Plan file, resulting in the number "LOCL425203".

3. Assign the different tag prefixes to different Trunk Groups in the Inbound IP Routing Table (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **IP to Trunk Group Routing**):
  - The Dest. Phone Prefix' field is set to the value "LOCL" and this rule is assigned to a local Trunk Group (e.g. Trunk Group ID 1).
  - The Dest. Phone Prefix' field is set to the value "LONG" and this rule is assigned to a long distance Trunk Group (e.g. Trunk Group ID 2).

**Figure 43-1: Configuring Dial Plan File Label for IP-to-Tel Routing**

<div> <div>Routing Index: 1-12</div> <div>IP To Tel Routing Mode: Route calls before manipulation</div> </div>						
	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Hunt Group ID
1			LOCL			1
2			LONG			2

The above routing rules are configured to be performed before manipulation (described in the step below).

4. Configure manipulation in the Destination Phone Number Manipulation Table for IP to Tel Calls table (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** submenu > **Dest Number IP->Tel**) for removing the first four characters of the called party number "tag" (in our example, "LOCL" and "LONG"):
- The Destination Prefix' field is set to the value "LOCL" and the 'Stripped Digits From Left' field is set to '4'.
  - The Destination Prefix' field is set to the value "LONG" and the 'Stripped Digits From Left' field is set to '4'.

**Figure 43-2: Configuring Manipulation for Removing Label**

Index	Destination Prefix	Source Prefix	Source IP Address	Stripped Digits From Left
1	LOCL	*	*	4
2	LONG	*	*	4

### 43.1.3.4 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 Tel-to-IP /IP-to-IP calls and SBC calls. This enables the mapping of called numbers to IP addresses (in dotted-decimal notation) or FQDNs (up to 15 characters).

➤ **To configure routing to an IP destination based on Dial Plan:**

1. Create the Dial Plan file. The syntax of the Dial Plan index for this feature is as follows:

```
<destination / called prefix number>,0,<IP destination>
```

Note that the second parameter "0" is not used and ignored.

An example of a configured Dial Plan (# 6) in the Dial Plan file is shown below:

```
[ PLAN6 ]
200,0,10.33.8.52      ; called prefix 200 is routed to
10.33.8.52
201,0,10.33.8.52
300,0,itsp.com       ; called prefix 300 is routed to itsp.com
```

2. Convert the file to a loadable file and then load it to the device.
3. Assign the Dial Plan index to the required routing rule:
  - 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.
  - Tel-to-IP or IP-to-IP Calls (Gateway/IP-to-IP application): In the Outbound IP Routing table, do the following:
    - ◆ In the 'Destination Address' field, enter the required Dial Plan index using the following syntax:

*DialPlan<index>*

Where "DialPlan0" denotes [PLAN1] in the Dial Plan file, "DialPlan1" denotes [PLAN2], and so on.



**Note:** The "DialPlan" string is case-sensitive.

### 43.1.3.5 Modifying ISDN-to-IP Calling Party Number

The device can use the Dial Plan file to change the Calling Party Number value (source number) of the incoming ISDN call when sending to IP. For this feature, the Dial Plan file supports the following syntax:

**<ISDN Calling Party Number>,0,<new calling number>**

- The first number contains the calling party number (or its prefix) received in the ISDN call SETUP message. The source number can also be a range, using the syntax [x-y] in the Dial Plan file. This number is used as the display name in the From header of the outgoing INVITE.
- The second number must always be set to "0".
- The third number is a string of up to 12 characters containing the mapped number that is used as the URI user part in the From and Contact headers of the outgoing INVITE.

The Dial Plan index used in the Dial Plan file for this feature is defined by the Tel2IPSourceNumberMappingDialPlanIndex parameter.

An example of such a configuration in the Dial Plan file is shown below:

```
[ PLAN1 ]
; specific received number changed to 04343434181.
0567811181,0,04343434181
; number range that changes to 04343434181.
056788118[2-4],0,04343434181
```

If we take the first Dial Plan rule in the example above (i.e., "0567811181,0,04343434181"), the received Calling Number Party of 0567811181 is changed to 04343434181 and sent to the IP with a SIP INVITE as follows:

```
Via: SIP/2.0/UDP 211.192.160.214:5060;branch=z9hG4bK3157667347
From: <sip:04343434181@kt.co.kr:5060>;tag=de0004b1
To: sip:01066557573@kt.co.kr:5060
Call-ID: 585e60ec@211.192.160.214
CSeq: 1 INVITE
Contact:<sip:04343434181@211.192.160.214:5060;transport=udp>
```

The initial Dial Plan text file must be converted to \*.dat file format using the DConvert utility. This is done by clicking the DConvert's **Process Dial Plan File** button. For more information, refer to *DConvert Utility User's Guide*.

You can load this \*.dat file to the device using the Web interface (see 'Loading Auxiliary Files' on page 535), AcBootP utility, or using the Auto-update mechanism from an external HTTP server.



#### Notes:

- Tel-to-IP routing is performed on the original source number if the parameter 'Tel to IP Routing Mode' is set to 'Route calls before manipulation'.
- Tel-to-IP routing is performed on the modified source number as defined in the Dial Plan file, if the parameter 'Tel To IP Routing Mode' is set to 'Route calls after manipulation'.
- Source number Tel-to-IP manipulation is performed on the modified source number as defined in the Dial Plan file.

### 43.1.4 User Information File

This section describes the various uses of the User Info file.

You can load the User Info file using any of the following methods:

- Web interface (see 'Loading Auxiliary Files' on page 535)
- *ini* file - using the UserInfoFileName parameter, e.g., UserInfoFileName = 'UserInformationFile.txt' (see 'Auxiliary and Configuration File Name Parameters' on page 893)
- Automatic update mechanism - using the UserInfoFileURL parameter, e.g., UserInfoFileUrl = 'http://192.168.0.250/Audiocodes/ UserInformationFile.txt' (see 'Automatic Update' on page 561)



**Note:** Instead of using a User Info file, you can configure the User Info table using the CLI, as described in 'Configuring User Info Table using CLI' on page 550.



#### 43.1.4.1 User Information File for PBX Extensions and "Global" Numbers

The User Info file contains a User Info table that can be used for the following Gateway-related:

- **Mapping (Manipulating) PBX Extension Numbers with Global Phone Numbers:** maps PBX extension number, connected to the device, with any "global" phone number (alphanumeric) for the IP side. In this context, the "global" phone number serves as a routing identifier for calls in the "IP world" and the PBX extension uses this mapping to emulate the behavior of an IP phone. This feature is especially useful in scenarios where unique or non-consecutive number translation per PBX is needed. This number manipulation feature supports the following call directions:

- **IP-to-Tel Calls:** Maps the called "global" number (in the Request-URI user part) to the PBX extension number. For example, if the device receives an IP call destined for "global" number 638002, it changes this called number to the PBX extension number 402, and then sends the call to the PBX extension on the Tel side.



**Note:** If you have configured regular IP-to-Tel manipulation rules (see 'Configuring Source/Destination Number Manipulation' on page 297), the device applies these rules before applying the mapping rules of the User Info table.

- **Tel-to-IP Calls:** Maps the calling (source) PBX extension to the "global" number. For example, if the device receives a Tel call from PBX extension 402, it changes this calling number to 638002, and then sends call to the IP side with this calling number. In addition to the "global" phone number, the display name (caller ID) configured for the PBX user in the User Info table is used in the SIP From header.



**Note:** If you have configured regular Tel-to-IP manipulation rules (see 'Configuring Source/Destination Number Manipulation' on page 297), the device applies these rules before applying the mapping rules of the User Info table.

- **IP-to-IP Calls:** Maps SIP From (calling number) and To (called number) of IP PBX extension numbers with "global" numbers. For example, if the device receives a call from IP PBX extension number 402 (calling / SIP From) that is destined to IP PBX extension number 403 (called / SIP To), the device changes both these numbers into their "global" numbers 638002 and 638003, respectively.

- **Registering Users:** The device can register each PBX user configured in the User Info table. For each user, the device sends a SIP REGISTER to an external IP-based Registrar server, using the "global" number in the From/To headers. If authentication is necessary for registration, the device sends the user's username and password, configured in the User Info table, in the SIP MD5 Authorization header.



**Notes:**

- To enable the User Info table, see 'Enabling the User Info Table' on page 551.
- To modify the Use Info table, you need to load a new User Info table containing your modifications. However, instead of loading a new User Info file, you can modify the User Info table using CLI, as described in 'Configuring User Info Table using CLI' on page 550.
- To enable user registration, set the following parameters on the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Proxy & Registration**) as shown:



- ✓ 'Enable Registration' parameter set to **Enable** (IsRegisterNeeded is set to 1).
- ✓ 'Registration Mode' parameter set to **Per Endpoint** (AuthenticationMode is set to 0).
- For FXS ports, when the device needs to send a new SIP request with the Authorization header (e.g., after receiving a SIP 401 response), it uses the username and password configured in the Authentication table (see 'Configuring Authentication per Port' on page 395). To use the username and password configured in the User Info file, set the 'Password' parameter to any value other than its default value.

The User Info file is a text-based file that you can create using any text-based program such as Notepad. To add mapping rules to this file, use the following syntax:

```
[ GW ]
FORMAT
PBXExtensionNum,GlobalPhoneNum,DisplayName,UserName,Password
```

Where:

- *PBXExtensionNum* is the PBX extension number (up to 10 characters)
- *GlobalPhoneNum* is the "global" phone number (up to 20 characters) for the IP side
- *DisplayName* is the Caller ID (string of up to 30 characters) of the PBX extension
- *UserName* is the username (string of up to 40 characters) for registering the user when authentication is necessary
- *Password* is the password (string of up to 20 characters) for registering the user when authentication is necessary

Each line in the file represents a mapping rule of a single PBX extension user.

You can add up to 1,000 mapping rules. The maximum size of the User Info file is 10,800 bytes for analog interfaces and 108,000 bytes for digital interfaces.



**Note:** Make sure that the last line in the User Info file ends with a carriage return (i.e., by pressing the <Enter> key).

An example of a configured User Info file is shown below:

```
[ GW ]
FORMAT
PBXExtensionNum,GlobalPhoneNum,DisplayName,UserName,Password
401 , 638001 , Mike , miked , 1234
402 , 638002 , Lee , leep, 4321
403 , 638003 , Sue , suer, 8790
404 , 638004 , John , johnd, 7694
405 , 638005 , Pam , pame, 3928
406 , 638006 , Steve , steveg, 1119
407 , 638007 , Fred , frede, 8142
408 , 638008 , Maggie , maggiew , 9807
```

#### 43.1.4.2 User Information File for SBC User Database

You can create a User Info table of SBC users from a loaded User Info file. This User Info file is the same file used for the GW / IP-to-IP application.

The device can use the SBC User Info for the following:

- Registering each user to an external registrar server.
- Authenticating (for any SIP request and as a client) each user if challenged by an external server.
- Authenticating as a server incoming user requests (for SBC security).

If the device registers on behalf of users and the users do not perform registration, any SIP request destined to the user is routed to the Proxy Set associated with the user's IP Group.

The User Info file is a text-based file that you can create using any text-based program such as Notepad. To add SBC users to this file, use the following syntax:

```
[ SBC ]
FORMAT LocalUser,UserName,Password,IPGroupID
john,john_user,john_pass,2
sue,sue_user,sue_pass,1
```

where:

- *LocalUser* is the user and is used as the Request-URI user part for the AOR in the database
- *UserName* is the user's authentication username
- *Password* is the user's authentication password
- *IPGroupID* is the IP Group ID to which the user belongs and is used as the Request-URI source host part for the AOR in the database



#### Notes:

- To enable the User Info table, see 'Enabling the User Info Table' on page 551.
- To modify the User Info table, you need to load a new User Info table containing your modifications. However, instead of loading a new User Info file, you can modify the User Info table using CLI, as described in 'Configuring User Info Table using CLI' on page 550.

### 43.1.4.3 Configuring User Info Table using CLI

Instead of using the User Info file to configure the Gateway and SBC User Info tables, you can configure these tables through CLI. The CLI lets you add, edit, delete, and search users in the User Info table.



#### Notes:

- If you load a User Info file to the device, all previous User Info table entries are deleted and replaced with the entries in the loaded User Info file.
- To enable the User Info table, see 'Enabling the User Info Table' on page 551.

The CLI path to these tables is as follows:

```
# configure voip
(config-voip)# sip-definition proxy-and-registration
(sip-def-proxy-and-reg)# user-info <gw-user-info (for Gateway) |
sbc-user-info (for SBC)>
```

The following commands can be used:

- To view all table entries, use the `display` command, as shown in the example below:

```
• SBC:
(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)

```

- **Gateway:**

```

(sip-def-proxy-and-reg)# user-info gw-user-info display
---- gw-user-info-0 ----
pbx-ext (405)
global-phone-num (405)
display-name (Ext405)
username (user405)
password (0aGzoKfh5uI=)
status (not-resgistered)

```

- To view a specific entry, enter the table index number and `display` command:

```

(sip-def-proxy-and-reg)# user-info sbc-user-info 1
(sbc-user-info-1)# display
local-user (SuePark)
username (userSue)
password (t6sn+un=)
ip-group-id (1)
status (not-resgistered)

```

- To add and/or define a user, use the `set` command, as shown in the example below:

```

(sip-def-proxy-and-reg)# user-info sbc-user-info 1
(sbc-user-info-1)# set username JohnDee

```

- To apply your changes, use the `exit` or `activate` command per user addition or modification (not per parameter):

```

(sbc-user-info-1)# <activate | exit>

```

- To search a user (by `pbx-ext` for Gateway or `local-user` for SBC), use the `find` command, as shown in the example below:

```

sip-def-proxy-and-reg)# user-info find <pbx-ext e.g., 300
local-user, e.g., JohnDoe>
JohnDee: Found at index 3 in SBC user info table, not
registered

```

The search locates the table index belonging to the searched user.

- To delete a user, use the `no` command, as shown in the example below:

```

(sip-def-proxy-and-reg)# no user-info sbc-user-info <database
index entry, e.g., 1>

```

#### 43.1.4.4 Enabling the User Info Table

The procedure below describes how to load a User Info file to the device and enable the use of the User Info table:

➤ **To enable the User Info table:**

4. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).
5. Set the 'Enable User-Information Usage' parameter to **Enable**.

## 43.2 Software License Key

The device is shipped with a pre-installed Software License Key, which determines the device's supported features, capabilities, and available resources. You can upgrade or change your device's supported features by purchasing and installing a new Software License Key to match your requirements.



**Note:** The availability of certain Web pages depends on the installed Software License Key.

### 43.2.1 Obtaining the Software License Key File

Before you can install a new Software License Key, you need to obtain a Software License Key file for your device with the required features from your AudioCodes representative. The Software License Key is an encrypted key in string format that is associated with the device's serial number ("S/N") and supplied in a text-based file.

If you need a Software License Key for more than one device, the Software License Key file can include multiple Software License Keys (see figure below). In such cases, each Software License Key in the file is associated with a unique serial number identifying the specific device. When loading such a Software License Key file, the device installs only the Software License Key that is associated with its serial number.

**Figure 3: Software License Key File with Multiple S/N Lines**



#### ➤ To obtain a Software License Key:

1. Make a note of the MAC address and/or serial number of the device:
  - a. Open the Device Information page (**Status & Diagnostics** tab > **System Status** menu > **Device Information**).
  - b. The MAC address is displayed in the "MAC Address" field and the serial number in the "Serial Number" field.
2. If you need a Software License Key for more than one device, repeat Step 1 for each device.
3. Request the required Software License Key from your AudioCodes representative and provide them with the MAC address and/or serial number of the device(s).
4. When you receive the new Software 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> = <Software 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 Software License Keys, ensure that each "S/N" value corresponds to a device.



**Warning:** Do not modify the contents of the Software License Key file.

5. Install the Software License Key on the device as described in 'Installing the Software License Key' on page 553.

### 43.2.2 Installing the Software License Key

Once you have received your Software License Key file from your AudioCodes representative, you can install it on the device using one of the following management tools:

- Web interface - see 'Installing the Software License Key using Web' on page 553
- CLI – see 'Installing the Software License Key using CLI' on page 554
- AudioCodes EMS - refer to the EMS User's Manual or EMS Product Description



**Note:** When you install a new Software License Key, it is loaded to the device's non-volatile flash memory and overwrites the previously installed Software License Key.

#### 43.2.2.1 Installing the Software License Key using Web

The procedure below describes how to install the Software License Key using the Web interface.

- **To install the Software License Key using the Web interface:**

1. Open the Software Upgrade Key Status page (**Maintenance** tab > **Software Update** menu > **Software Upgrade Key**).

Current Key: ISN2r5toqBQ8bBt581xJu6i9j3Zcf3ta41wnehcs8hofalNeb1b1R5ZPFQ9ncypf5xZAixcs8xfamhSah4Za2c

Key features:  
 Board Type: Mediant 800 - MSBG  
 Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol  
 Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727 ILBC EVRC-B  
 AMR-WB G722 EG711 MS\_RTA\_NB MS\_RTA\_WB SILK\_NB SILK\_WB  
 QOE features: VoiceQualityMonitoring MediaEnhancement  
 PSTN FALLBACK Supported  
 DSP Voice features: RTCP-XR AMRPolicyManagement V150=1  
 E1Trunks=4  
 T1Trunks=4  
 EvsPorts=8

Add a Software Upgrade Key

Load "Upgrade Key" file from your computer to the device

Browse... Load File

Reset with flash burn is required after file is loaded.

2. As a precaution, backup the Software License Key currently installed on the device. If the new Software License Key does not comply with your requirements, you can re-load this backup to restore the device's original capabilities.
  - a. In the 'Current Key' field, select the entire text string and copy it to any standard text file (e.g., Notepad).
  - b. Save the text file with any file name and file extension (e.g., key.txt) to a folder on your computer.
3. Depending on whether you are loading a Software License Key file with a single Software License Key (i.e., one "S/N") or with multiple Software License Keys (i.e., more than one "S/N"), do one of the following:
  - **Loading a File with a Single Software License Key:**
    - a. Open the Software License Key file using a text-based program such as Notepad.
    - b. Copy-and-paste the string from the file to the 'Add a Software Upgrade Key' field.
    - c. Click the **Add Key** button.
  - **Loading a File with Multiple Software License Keys:**
    - a. In the 'Load Upgrade Key file ...' field, click the **Browse** button and navigate to the folder in which the Software License Key file is located on your computer.
    - b. Click **Load File**; the new key is installed on the device.

If the Software License Key is valid, it is burned to the device's flash memory and displayed in the 'Current Key' field.
4. Verify that the Software License Key was successfully installed, by doing one of the following:
  - In the Software Upgrade Key Status page, check that the listed features and capabilities activated by the installed Software License Key match those that were ordered.
  - Access the Syslog server and ensure that the following message appears in the Syslog server:  
"S/N\_\_\_ Key Was Updated. The Board Needs to be Reloaded with ini file\n"
5. Reset the device; the new capabilities and resources enabled by the Software License Key are active.



**Note:** If the Syslog server indicates that the Software License Key was unsuccessfully loaded (i.e., the "SN\_" line is blank), do the following preliminary troubleshooting procedures:

1. Open the Software License Key file and check that the "S/N" line appears. If it does not appear, contact AudioCodes.
2. Verify that you have loaded the correct file. Open the file and ensure that the first line displays "[LicenseKeys]".
3. Verify that the content of the file has not been altered.

#### 43.2.2.2 Installing the Software License Key using CLI

To install the Software License Key using CLI, use the following commands:

- To install the Software License Key:  

```
(config-system)# feature-key
```
- To view the Software License Key:  

```
show system feature-key
```

## 43.3 Software Upgrade Wizard

The Software Upgrade Wizard allows you to upgrade the device's firmware. The firmware file has the .cmp file extension name. The wizard also enables you to load an *ini* file and/or auxiliary files (typically loaded using the Load Auxiliary File page described in 'Loading Auxiliary Files' on page 535). However, it is mandatory when using the wizard to first load a .cmp file to the device. You can then choose to also load an *ini* file and/or auxiliary files, but this cannot be done without first loading a .cmp file. For the *ini* and each auxiliary file type, you can choose to load a new file or not load a file but use the existing file (i.e., maintain existing configuration) running on the device.



**Warning:** The Software Upgrade Wizard requires the device to be reset at the end of the process, which may disrupt traffic. To avoid this, disable all traffic on the device before initiating the wizard by performing a graceful lock (see 'Basic Maintenance' on page 529).



**Notes:**

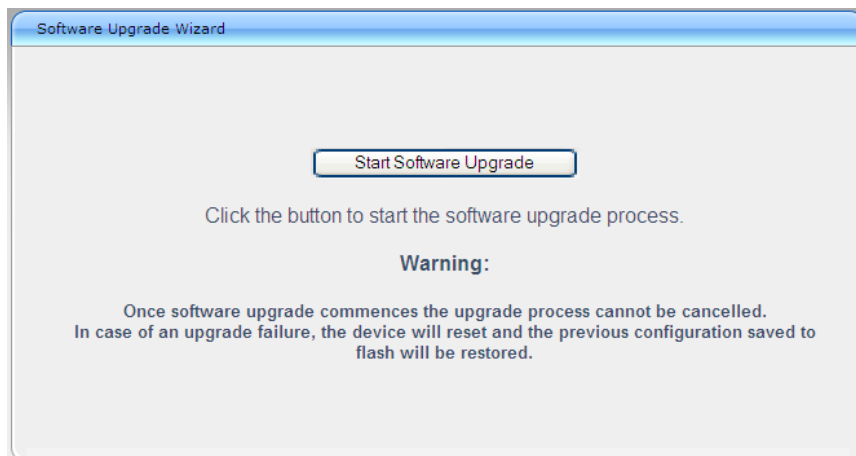
- You can get the latest software files from AudioCodes Web site at <http://www.audiocodes.com/downloads>.
- Before upgrading the device, it is recommended that you save a copy of the device's configuration settings (i.e., *ini* file and data file) to your computer. If an upgrade failure occurs, you can then restore your configuration settings by uploading the backup file to the device. For saving and restoring configuration, see 'Backing Up and Loading Configuration File' on page 558.
- If you wish to also load an *ini* or auxiliary file, it is mandatory to first load a .cmp file.
- When you activate the wizard, the rest of the Web interface is unavailable. After the files are successfully loaded, access to the full Web interface is restored.
- If you upgraded your .cmp and the "SW version mismatch" message appears in the Syslog or Web interface, then your Software License Key does not support the new .cmp file version. If this occurs, contact AudioCodes support for assistance.
- If you use the wizard to load an *ini* file, parameters excluded from the *ini* file are assigned default values (according to the .cmp file running on the device) thereby, overriding values previously defined for these parameters.
- You can schedule automatic loading of these files using HTTP/HTTPS (see 'Automatic Update' on page 561).
- You can also upgrade the device's firmware by loading a .cmp file from an external USB hard drive connected to the device's USB port. For more information, see USB Storage Capabilities on page 573.



➤ **To load files using the Software Upgrade Wizard:**


1. Stop all traffic on the device using the Graceful Lock feature (refer to the warning bulletin above).
2. Open the Software Upgrade wizard, by performing one of the following:
  - Select the **Maintenance** tab, click the **Software Update** menu, and then click **Software Upgrade Wizard**.
  - On the toolbar, click **Device Actions**, and then choose **Software Upgrade Wizard**.


**Figure 43-4: Start Software Upgrade Wizard Screen**



3. Click the **Start Software Upgrade** button; the wizard starts, requesting you to browse to a .cmp file for uploading.




**Note:** At this stage, you can quit the Software Update Wizard, by clicking **Cancel** , without requiring a device reset. However, once you start uploading a cmp file, the process must be completed with a device reset. If you choose to quit the process in any of the subsequent pages, the device resets.





4. Click the **Browse** button, navigate to the .cmp file, and then click **Load File**; a progress bar appears displaying the status of the loading process. When the .cmp file is successfully loaded to the device, a message appears notifying you of this.
5. If you want to load **only** a .cmp file, then click the **Reset**  button to reset the device with the newly loaded .cmp file, utilizing the existing configuration (*ini*) and auxiliary files. To load additional files, skip to the next Step.



**Note:** Device reset may take a few minutes depending on cmp file version (this may even take up to 10 minutes).

6. Click the **Next**  button; the wizard page for loading an *ini* file appears. You can now perform one of the following:
  - Load a new *ini* file: Click **Browse**, navigate to the *ini* file, and then click **Send File**; the *ini* file is loaded to the device and you're notified as to a successful loading.



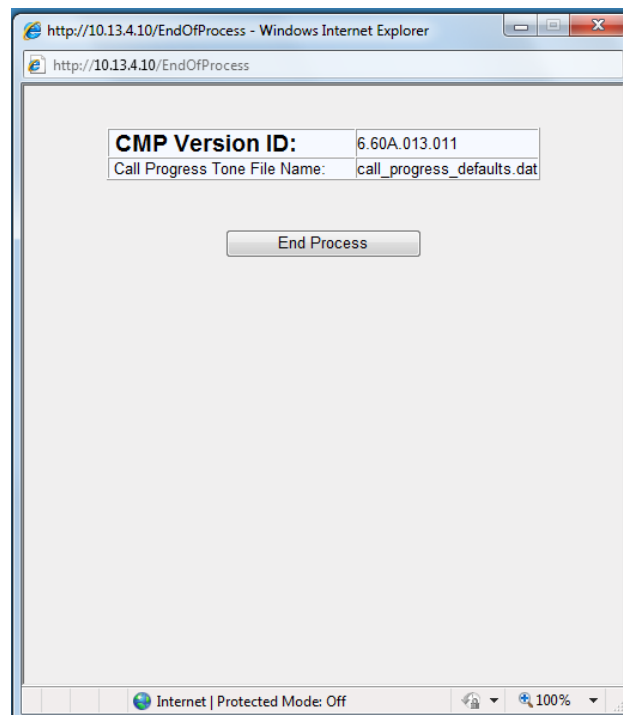
- Retain the existing configuration (*ini* file): Do not select an *ini* file, and ensure that the 'Use existing configuration' check box is selected (default).
  - Return the device's configuration settings to factory defaults: Do not select an *ini* file, and clear the 'Use existing configuration' check box.
7. Click the **Next**  button to progress to the relevant wizard pages for loading the desired auxiliary files. To return to the previous wizard page, click the **Back**  button. As you navigate between wizard pages, the relevant file type corresponding to the Wizard page is highlighted in the left pane.
  8. When you have completed loading all the desired files, click the **Next**  button until the last wizard page appears ("FINISH" is highlighted in the left pane).
  9. Click the **Reset**  button to complete the upgrade process; the device 'burns' the newly loaded files to flash memory and then resets the device.



**Note:** Device reset may take a few minutes (depending on .cmp file version, this may even take up to 30 minutes).

After the device resets, the End of Process wizard page appears displaying the new .cmp and auxiliary files loaded to the device.

**Figure 43-5: Software Upgrade Process Completed Successfully**



10. Click **End Process** to close the wizard; the Web Login dialog box appears.
11. Enter your login user name and password, and then click **OK**; a message box appears informing you of the new .cmp file.
12. Click **OK**; the Web interface becomes active, reflecting the upgraded device.

## 43.4 Backing Up and Loading Configuration File

You can save a copy/backup of the device's current configuration settings as an *ini* file to a folder on your computer, using the Configuration File page. The saved *ini* file includes only parameters that were modified and parameters with other than default values. The Configuration File page also allows you to load an *ini* file to the device. If the device has "lost" its configuration, you can restore the device's configuration by loading the previously saved *ini* file or by simply loading a newly created *ini* file.



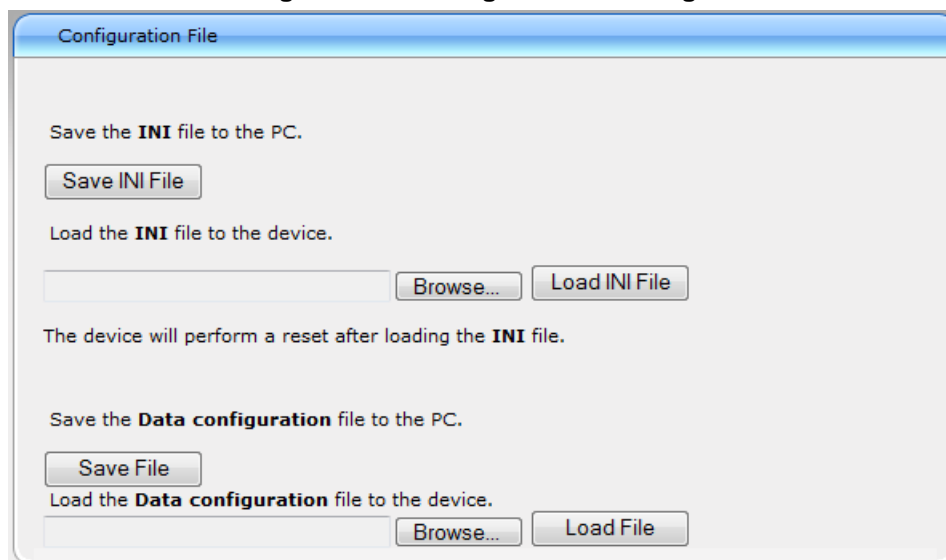
### Notes:

- When loading an *ini* file using this Web page, parameters not included in the *ini* file are reset to default settings.
- You can also save the current configuration to and update configuration from an external USB hard drive connected to the device's USB port. For more information, see USB Storage Capabilities on page 573.

### ➤ To save the *ini* / data file:

1. Open the Configuration File page by doing one of the following:
  - From the Navigation tree, click the **Maintenance** tab, click the **Software Update** menu, and then click **Configuration File**.
  - On the toolbar, click **Device Actions**, and then from the drop-down menu, choose **Load Configuration File** or **Save Configuration File**.

Figure 43-6: Configuration File Page



2. To save the Voice *ini* file to a folder on your computer, do the following:
  - a. Click the **Save INI File** button; the File Download dialog box appears.
  - b. Click the **Save** button, navigate to the folder where you want to save the *ini* file, and then click **Save**.
3. To save the Data configuration ini file to a folder on your computer, do the following:
  - a. Under the 'Save the Data configuration file to the PC' group, click the Save File button; the 'File Download' dialog box appears.
  - b. Click the Save button, navigate to the folder in which you want to save the file on your PC, and then click Save; the device saves the Data ini file to the selected folder.

4. To load the Voice *ini* file to the device, do the following:
  - a. Click the **Browse** button, navigate to the folder where the *ini* file is located, select the file, and then click **Open**; the name and path of the file appear in the field beside the **Browse** button.
  - b. Click the **Load INI File** button, and then at the prompt, click **OK**; the device uploads the *ini* file and then resets (from the *cmp* version stored on the flash memory). Once complete, the Web Login screen appears, requesting you to enter your user name and password.
5. To load the Data configuration ini file to the device, do the following:
  - a. Under the 'Send the Data Configuration file to the device' group, click the Browse button, navigate to the folder in which the file is located, select the file, and then click Open; the name and path of the file appear in the field beside the Browse button.
  - b. Click the Load File button, and then at the prompt, click OK; the device uploads the file and then resets (from the *cmp* version stored on the flash memory). Once complete, the Web Login screen appears, requesting you to enter your user name and password.

## Reader's Notes

## 44 Automatic Update

Automatic provisioning is useful for large-scale deployment of devices. In some cases, the devices are shipped to the end customer directly from the manufacturer. In other cases, they may pass through a staging warehouse. Configuration may occur at the staging warehouse or at the end-customer premises.

The devices may be pre-configured during the manufacturing process (commonly known as *private labeling*). Typically, a two-stage configuration process is implemented such that initial configuration includes only basic configuration, while the final configuration is done when the device is deployed in a live network. In addition, the devices may be deployed without configuration and then automatically provisioned by triggering the Automatic Update feature using the Zero Configuration mechanism (see [Configuring Zero Configuration](#) on page 568).

Automatic provisioning can be used to update the following files:

- Software file (*cmp*)
- Auxiliary files (e.g., Call Progress Tones)
- Configuration file

The configuration file can be one of the following types, depending on required configuration:

- ini File: File containing ini file parameters only, which configures only System and VoIP functionalities.
- CLI script file: File containing CLI commands only. This can be used for configuring all the device's functionalities (i.e., System, VoIP, and Data Routing). You can use one of the following types of CLI script files, the only difference being in the way they configure the device:
  - ◆ CLI script file: This file updates the device's configuration only according to the file's configuration settings. The device's other existing configuration settings (not included in the file) are retained. The URL of the server where this file is located is configured by the AUPDCliScriptURL parameter.
  - ◆ Startup CLI script file: This file updates the device's configuration according to the file's configuration settings and sets all other parameters that were not included in the file to factory defaults. This script file causes two device resets. The URL of the server where this file is located is configured by the AUPDStartupScriptURL parameter.



Notes:

- The CLI script files can have any filename extension.
- If a device reset is required to apply certain configuration settings, you can include the following CLI command in the CLI script file: reload if-needed. This command must be added at the end of the file.

The Automatic Update mechanism is applied per file, using specific parameters that define the URLs to the servers where the files are located, and the file names (see [Automatic Update Parameters](#) on page 894). These files can be stored on any standard Web, FTP, or NFS server and can be loaded periodically to the device using HTTP, HTTPS, FTP, or NFS. This mechanism can be used even for devices that are installed behind NAT and firewalls.

The Automatic Update mechanism can be triggered by the following:

- Upon device startup.
- At a user-defined time of day (e.g., 18:00), configured by the *ini* file parameter AutoUpdatePredefinedTime.

- Periodically (e.g., every 60 minutes), configured by the *ini* file parameter `AutoUpdateFrequency`.
- Upon startup but before the device is operational, if the Secure Startup feature is enabled (see 'Loading Files Securely by Disabling TFTP' on page 566).
- Upon receipt of a special SIP Notify message (see 'Remotely Triggering Auto Update using SIP NOTIFY' on page 567)

When implementing Automatic Updates using HTTP/S, the device determines whether the file on the provisioning server is an updated one as follows:

- **Configuration file:** The device checks the timestamp according to the HTTP server response. Cyclical Redundancy Check (CRC) is only checked if the `AUPDCheckIfIniChanged` parameter is enabled. The device downloads the configuration file only if it was modified since the last successful configuration update.
- **Software file (cmp):** The device first downloads the file and then checks if its version number is different from the software version file currently stored on the device's flash memory.
- **Auxiliary files (e.g., CPT):** These files are updated only once. To update the auxiliary file again, you must modify the settings of the related parameter that configures its URL.

## 44.1 Configuring Automatic Update

The procedure below describes how to configure the Automatic Update feature. It describes a scenario where the devices download a "master" configuration file with common settings from an HTTP server. This "master" file applies common configuration and instructs each device to download a specific configuration file based on the device's MAC address from an HTTP server.



**Warning:** Do not use the Web interface to configure the device when the Automatic Update feature is implemented. If you do and save (burn) the new settings to the device's flash memory, the `IniFileURL` parameter is automatically set to 0 and Automatic Updates is consequently disabled. To enable Automatic Updates again, you would need to re-load the ini file (using the Web interface or BootP) with the correct `IniFileURL` settings. As a safeguard to an unintended burn-to-flash when resetting the device, if the device is configured for Automatic Updates, the 'Burn To FLASH' field under the Reset Configuration group in the Web interface's Maintenance Actions page is automatically set to **No** by default.



### Notes:

- For a description of all the Automatic Update *ini* file parameters, see Automatic Update Parameters on page 894.
- For a description of the CLI parameters relating to Automatic Update, refer to the *MSBR Series CLI Reference Guide for System and VoIP Functionalities*.

### ➤ To configure the Automatic Update feature (ini file example):

1. Setup a Web server (e.g., `http://www.corp.com`) and place all the required configuration files on this server.
2. For each device, preconfigure the following parameter (DHCP / DNS are assumed):

```
IniFileURL = 'http://www.corp.com/master_configuration.ini'
```

3. Create a file named *master\_configuration.ini* with the following text:

```
# Common configuration for all devices
# -----
CptFileURL = 'http://www.corp.com/call_progress.dat'
# Check for updates every 60 minutes
AutoUpdateFrequency = 60
# Additional configuration per device
# -----
# Each device loads a file named based on its MAC address
# (e.g., config_00908F033512.ini)
IniFileURL = 'http://www.corp.com/config_<MAC>.ini'
# Reset the device after configuration is updated.
# The device resets after all files are processed.
ResetNow = 1
```

You can modify the *master\_configuration.ini* file (or any of the *config\_<MAC>.ini* files) at any time. The device queries for the latest version every 60 minutes and applies the new settings immediately.

4. For additional security, use HTTPS or FTPS. The device supports HTTPS (RFC 2818) and FTPS using the AUTH TLS method <draft-murray-auth-ftp-ssl-16>.
5. To download configuration files from an NFS server, the NFS file system parameters should be defined in the *ini* file. The following is an example of an *ini* file for downloading files from NFS servers using NFS version 2:

```
# Define NFS servers for Automatic Update
[ NFSServers ]
FORMAT NFSServers_Index = NFSServers_HostOrIP,
NFSServers_RootPath, NFSServers_NfsVersion;
NFSServers 1 = 10.31.2.10, /usr/share, 2 ;
NFSServers 2 = 192.168.100.7, /d/shared, 2 ;
[ \NFSServers ]
CptFileUrl =
'file://10.31.2.10/usr/share/public/usa_tones.dat'
VpFileUrl =
'file://192.168.100.7/d/shared/gateways/voiceprompt.dat'
```

The following *ini* file example can be used to activate the Automatic Update mechanism.

```
# DNS is required for specifying domain names in URLs
[ InterfaceTable ]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingInterface;
InterfaceTable 0 = 6, 10, 10.13.4.12, 16, 10.13.0.1, 1, Mng,
10.1.1.11, 0.0.0.0, ;
[ \InterfaceTable ]
# Load an extra configuration ini file using HTTP
IniFileURL = 'http://webserver.corp.com/Gateway/inifile.ini'
# Load Call Progress Tones file using HTTPS
CptFileUrl = 'https://10.31.2.17/usa_tones.dat'
# Load Voice Prompts file using FTPS with user 'root' and password
'wheel'
VPFileUrl = 'ftps://root:wheel@ftpserver.corp.com/vp.dat'
# Update every day at 03:00 AM
AutoUpdatePredefinedTime = '03:00'
```

```
# Note: The cmp file isn't updated since it's disabled by default (AutoUpdateCmpFile).
```



#### Notes:

- The Automatic Update mechanism assumes that the external Web server conforms to the HTTP standard. If the Web server ignores the If-Modified-Since header, or doesn't provide the current date and time during the HTTP 200 OK response, the device may reset itself repeatedly. To overcome this problem, modify the update frequency, using the AutoUpdateFrequency parameter.
- To load a different configuration file (ini file) per device, add the string "<MAC>" to the URL (e.g., IniFileURL = 'http://www.corp.com/config\_<MAC>.ini'). This mnemonic is replaced with the device's hardware MAC address, resulting in an ini file name request that contains the device's MAC address (e.g., config\_00908F033512.ini).
- To prevent the device from accidentally upgrading its software, by default the Automatic Update feature does not apply a downloaded *cmp* file even if its URL was configured (using the CmpFileURL parameter). To enable this, set the AutoUpdateCmpFile parameter to 1.
- To enable the device to automatically reset after an ini file has been loaded, set the ResetNow parameter to 1. This is important if the downloaded configuration file includes parameters that require a device reset for its settings to be applied.
- By default, parameters that are not included in the downloaded configuration file are set to default. To retain the current settings of these parameters, set the SetDefaultOnINIFileProcess parameter to 0.

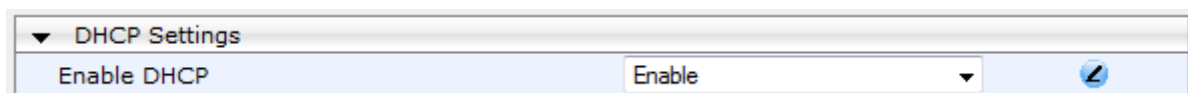
## 44.2 Obtaining IP Address Automatically using DHCP

You can configure the device to obtain an IP address from a DHCP server during bootup.

### ➤ To enable DHCP for obtaining an IP address:

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

Figure 44-1: Enabling DHCP - Application Settings Page



2. From the 'Enable DHCP' drop-down list, select **Enable**.
3. Click **Submit**.



**Note:** When using DHCP to acquire an IP address, the Multiple Interface table, VLANs and other advanced configuration options are disabled.



## 44.3 Automatic Configuration Methods

This section describes available methods that can be used for automatic device configuration.

### 44.3.1 DHCP-based Configuration Server

The DHCP server can be configured to automatically provide each device with a temporary IP address so that individual MAC addresses are not required. Configuration occurs at a staging warehouse for this method.

Below is an example configuration file for Linux DHCP server (dhcpd.conf). The devices are allocated temporary IP addresses in the range 10.31.4.53 to 10.31.4.75. TFTP is assumed to be on the same computer as the DHCP server (alternatively, the "next-server" directive may be used).

```
ddns-update-style ad-hoc;
default-lease-time 60;
max-lease-time 60;
class "gateways" {
    match if(substring(hardware, 1, 3) = 00:90:8f);
}
subnet 10.31.0.0 netmask 255.255.0.0 {
    pool {
        allow members of "audiocodes";
        range 10.31.4.53 10.31.4.75;
        filename "SIP_F6.60A.217.003.cmp -fb;device.ini";
        option routers                10.31.0.1;
        option subnet-mask            255.255.0.0;
    }
}
```

### 44.3.2 HTTP-based Automatic Updates

An HTTP/S server can be placed in the customer's network where configuration and software updates are available for download. This does not require additional servers at the customer premises and is NAT-safe.

For example, assume the core network HTTPS server is <https://www.corp.com>. A master configuration *ini* file should be placed on the server, e.g., <https://www.corp.com/gateways/master.ini>. This file could point to additional *ini* files, auxiliary files (e.g., call progress tones), and software files (cmp), all on the same HTTP server or different HTTP servers in the network.

The main advantage of this method is that the HTTP configuration can be checked periodically when the device is deployed at the customer site. HTTP(S) is not sensitive to NAT devices, enabling configuration whenever needed without on-site intervention.

For additional security, the URL may contain a different port, and username and password.

The devices should only be pre-configured with the URL of the initial *ini* file, using one of the following methods:

- Methods described in 'DHCP-based Configuration Server' on page 565 or above, via TFTP at a staging warehouse. The configuration URL is configured using the IniFileURL parameter.
- Private labeling.
- Manually on-site, using the RS-232 port or Web interface.

When the device is deployed at the customer site, local DHCP server provides the devices with IP addressing and DNS server information. From the URL provided in the DHCP

response, the device can then contact the HTTP server at the core network and automatically download its configuration. The URL can be a simple file name or contain the device's MAC or IP address, e.g.:

- `http://corp.com/config-<MAC>.ini` - which becomes, for example, `http://corp.com/config-00908f030012.ini`
- `http://corp.com/<IP>/config.ini` - which becomes, for example, `http://corp.com/192.168.0.7/config.ini`

### 44.3.3 Configuration using FTP or NFS

Some networks block access to HTTP(S). The Automatic Update feature provides limited support for FTP/FTPS connectivity. Periodic polling for updates is not possible since these protocols don't support conditional fetching, i.e., updating files only if it is changed on the server.

The only difference between this method and those described in 'HTTP-based Automatic Updates' on page 565 is that the protocol in the URL is "ftp" (instead of "http").



#### Notes:

- Unlike FTP, NFS is not NAT-safe.
- NFS v2/v3 is also supported.

### 44.3.4 Configuration 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.

## 44.4 Loading Files Securely by Disabling TFTP

The TFTP protocol is not considered secure and some network operators block it using a firewall. It is possible to disable TFTP completely, using the *ini* file parameter `EnableSecureStartup` (set to 1). This way, secure protocols such as HTTPS may be used to fetch the device configuration.

#### ➤ To download the ini file to the device using HTTPS instead of TFTP:

1. Prepare the device's configuration file on an HTTPS server and obtain a URL to the file (e.g., `https://192.168.100.53/gateways.ini`).
2. Enable DHCP, if necessary.
3. Enable SSH and connect to it.
4. In the CLI, use the *ini* file parameters `IniFileURL` (for defining the URL of the configuration file) and `EnableSecureStartup` (for disabling TFTP), and then restart the device with the new configuration:

```
/conf/scp IniFileURL https://192.168.100.53/gateways.ini
/conf/scp EnableSecureStartup 1
/conf/sar bootp
```



**Note:** Once Secure Startup has been enabled, it can only be disabled by setting `EnableSecureStartup` to 0 using the CLI. Loading a new *ini* file using BootP/TFTP is not possible until `EnableSecureStartup` is disabled.

## 44.5 Remotely Triggering Auto Update using SIP NOTIFY

The device can be remotely triggered to start the Automatic Update process upon receipt of a SIP NOTIFY that includes an Event header set to 'check-sync;reboot=false', as shown in the example below:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
From: sip:sipsak@<srchost>
CSeq: 10 NOTIFY
Call-ID: 1234@<srchost>
Event: check-sync;reboot=false
```

For this feature to function, Automatic Update must be enabled on the device. In other words, it must have a loaded ini file with the Automatic Update settings.

➤ **To enable remote trigger of Auto Update upon receipt of SIP NOTIFY:**

1. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).
2. Under the **Misc Parameters** group, set the 'SIP Remote Reset' parameter to **Enable**.
3. Click **Submit**.



**Notes:**

- This SIP Event header value is proprietary to AudioCodes.
- This feature does not trigger the Zero Configuration feature.

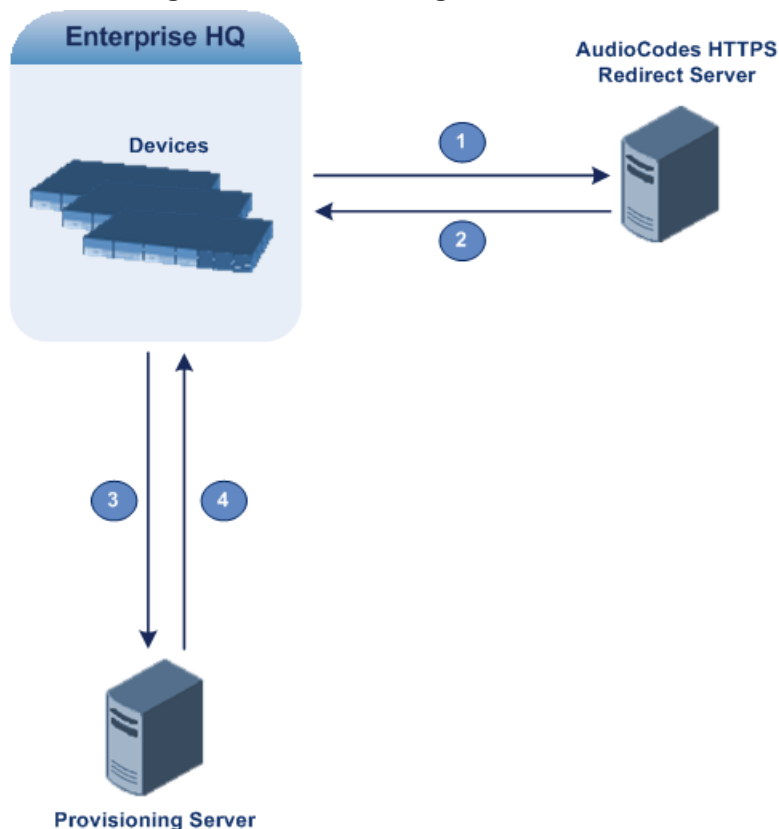
## 44.6 Configuring Zero Configuration

The Zero Configuration feature enables automatic, remote configuration of newly deployed, non-configured devices, using AudioCodes HTTPS Redirect Server. This feature offers an almost plug-and-play experience for quick-and-easy initial deployment of multiple devices at the end-customer premises. Zero Configuration requires only minimal preconfiguration of the device for WAN connectivity. Once an Internet connection is established, all that is needed is a device reset to activate the Zero Configuration mechanism.

Zero Configuration operates in combination with the Automatic Update feature. It redirects the device to an HTTP/S provisioning server from where the configuration file, configured with Automatic Update settings, can be downloaded and applied to the device. The device then performs the regular Automatic Update process according to these Automatic Update settings.

Once the device is powered up and connectivity to the WAN established, it automatically sends an HTTP request to AudioCodes HTTPS Redirect server. If the device's MAC address is listed on the server, the server responds to the device with an HTTP Redirect response containing the URL of the HTTP/S server (typically, a provisioning server maintained by the Service Provider) where the configuration file is located. The device then downloads the configuration file from this provisioning server and updates its configuration. Typically, this configuration file only enables the Automatic Update mechanism and therefore, once downloaded, the device executes the Automatic Update mechanism accordingly.

**Figure 44-2: Zero Configuration Process**



1. Device sends HTTPS request to AudioCodes HTTPS Redirect server.
2. Redirect server sends HTTPS response with redirect URL.
3. Device sends HTTPS request to redirected URL (i.e., provisioning server).
4. Device downloads configuration file for enabling the regular Automatic Update feature.

The configuration file contains only CLI commands for configuration, which its settings are applied to the device, in addition to the device's current configuration. The device resets only if the configuration file contains an explicit command instructing it to reset.

To enable Zero Configuration, the customer needs to define the devices on the HTTPS Redirect server by entering their MAC addresses and the configuration file URL. This may be done either through the corresponding Web interface or through SOAP/XML interface (that may be integrated with the Service Provider's provisioning system). For more information, contact AudioCodes support.

If the regular Automatic Update process succeeds, the device repeats the Zero Configuration process **only** if it undergoes a reset to factory defaults. If the Automatic Update process fails, the device repeats the Zero Configuration process at the next device reset or power up.

For security, communication between the device and the HTTPS Redirect server is encrypted (HTTPS) and setup with mutual authentication. The device uses a special factory-set certificate to authenticate itself with the HTTPS Redirect server and to verify authenticity of the latter. If the redirect URL (where the configuration file is stored) also uses the HTTPS protocol, the device can use a regular certificate or the Zero Configuration certificate to authenticate itself and validate the server's certificate if a trusted root certificate (regular) is configured. This is determined by the `AupdUseZeroConfCerts` parameter.

**Notes:**

- If the Automatic Update feature has been configured, the Zero Configuration process is performed first. Only after Zero Configuration completes (successfully or not), does the Automatic Update process begin.
- If the device is configured with multiple WAN interfaces, Zero Configuration is attempted on all configured WAN interfaces, sequentially.
- The recommended method for using both Zero Configuration and Automatic Update is as follows:
  - ✓ Zero Configuration is done to redirect the non-configured device to the URL of the provisioning server which contains only the configuration for the Automatic Update feature (e.g., CLI script URL and timeout for periodic update check).
  - ✓ Once the Zero Configuration process completes (i.e., the device has downloaded the configuration file and applied the Automatic Update settings) without undergoing a reset, the Automatic Update mechanism begins.

➤ **To set up and activate Zero Configuration:**

1. Configure the HTTPS Redirect server with the following:
  - MAC addresses of the devices you want to provision.
  - Redirect URL of the provisioning server where the configuration file with the Automatic Update settings is located.
  - Name of the configuration file.
2. Establish a CLI session with the device and configure Zero Configuration:
  - a. Enable Zero Configuration (default), by running the following command:

```
# configure system
(config-system)# automatic-update
(automatic-update)# set zero-conf <on|off>
```
  - b. Configure the URL of AudioCodes HTTPS Redirect server, by running the following command:

```
(automatic-update)# set zero-conf-server <URL>
```

The default URL is `https://redirect.audiocodes.com/<MAC address>`.
3. Create a CLI-based configuration file with settings relating to the Automatic Update feature (see 'Configuring Automatic Update' on page [562](#)) and place it on the HTTP/S redirected provisioning server.
4. Place the configuration, software (cmp), and/or auxiliary files on a provisioning server. This server can be the same provisioning server or any other server(s).
5. Configure the device's WAN interface and cable the device to the WAN network.
6. Power down and then power up the device.

## 45 Restoring Factory Defaults

You can restore the device's configuration to factory defaults using one of the following methods:

- CLI (see 'Restoring Defaults using CLI' on page [571](#))
- Hardware reset pinhole button (see Restoring Defaults using Hardware Reset Button on page [572](#))
- Loading an empty *ini* file (see 'Restoring Defaults using an ini File' on page [572](#))

### 45.1 Restoring Defaults using CLI

The device can be restored to factory defaults using CLI, as described in the procedure below.

➤ **To restore factory defaults using CLI:**

1. Access the CLI:
  - a. Connect the RS-232 serial port of the device to the communication port on your computer. For serial cabling, refer to the *Hardware Installation Manual*.
  - b. Establish serial communication with the device using a serial communication program (such as HyperTerminal™) with the following communication port settings:
    - ◆ **Baud Rate:** 115,200 bps
    - ◆ **Data Bits:** 8
    - ◆ **Parity:** None
    - ◆ **Stop Bits:** 1
    - ◆ **Flow Control:** None
2. At the CLI prompt, type the username (default is "Admin" - case sensitive), and then press Enter:

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

```
# Password: Admin
```
4. At the prompt, type the following, and then press Enter:

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

```
# Password: Admin
```
6. At the prompt, type the following to reset the device to default settings, and then press Enter:

```
# write factory
```

## 45.2 Restoring Defaults using Hardware Reset Button

The device's hardware reset pinhole button can be used to reset the device to default settings.

➤ **To restore default settings using the hardware reset pinhole button:**

- With a paper clip or any other similar pointed object, press and hold down the reset pinhole button, located on the front panel for at least 12 seconds (but no more than 25 seconds).

## 45.3 Restoring Defaults using an ini File

You can restore the device to factory default settings by loading an empty *ini* file to the device. This is done using the Web interface's Configuration File page (see 'Backing Up and Loading Configuration File' on page 558). If the *ini* file does include content (e.g., parameters), ensure that they are on lines beginning with comment signs (i.e., semicolons ";") so that the device ignores them.



**Note:** The only settings that are not restored to default are the management (OAMP) LAN IP address and the Web interface's login user name and password.



## 46 USB Storage Capabilities

The device enables USB storage using an external USB hard drive or flash disk (disk on key) connected to its USB port. The storage capabilities include the following:

- Saving network captures to the USB, using the following CLI command:  

```
# debug capture data physical stop usb
```
- Updating the device's firmware from the USB, using the following CLI command:  

```
# copy firmware from usb://<the .cmp file name>
```
- Updating the device's configuration from the USB, using the following CLI command:  

```
# copy voice-configuration from usb://<the .ini configuration file name>
```
- Saving current configuration to the USB, using the following CLI command:  

```
# copy voice-configuration to usb://<the .ini configuration file name>
```



**Note:** Only a single USB storage (formatted to FAT/FAT32) operation is supported at any given time.

## Reader's Notes

# **Part XII**

## **Status, Performance Monitoring and Reporting**



## 47 System Status

This section describes how to view various system statuses.

### 47.1 Viewing Device Information

The Device Information page [displays](#) various hardware and software information of the device. This page also lists any Auxiliary files that have been installed on the device and allows you to remove them.

➤ **To access the Device Information page:**

- Open the Device Information page (**Status & Diagnostics** tab > **System Status** menu > **Device Information**).

▼ General Settings	
MAC Address:	00908f26c975
Serial Number:	2541941
Board Type:	Mediant 800 - MSBG
Device Up Time:	8d:2h:23m:44s:8th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size [Mbytes]:	64
RAM Size [Mbytes]:	367
CPU Speed [MHz]:	500
▼ Versions	
Version ID:	6.60A.012.002
DSP Type:	1
DSP Software Version:	66015
DSP Software Name:	5014AE3_R_LD
Flash Version:	610
▼ Loaded Files	
Call Progress Tones File Name:	usa_tones_11.dat <span>Delete</span>
Loaded Coder Table :	Default CODERTABLE

➤ **To delete a loaded file:**

- Click the **Delete** button corresponding to the file that you want to delete. Deleting a file takes effect only after device reset (see 'Resetting the Device' on page [529](#)).

### 47.2 Viewing Ethernet Port Information

The Ethernet Port Information page [displays](#) read-only information on the Ethernet port connections. This includes information such as activity status, duplex mode, and speed as well as PoE.



**Note:** The Ethernet Port Information page [can](#) also be accessed from the Home page (see 'Viewing the Home Page' on page [54](#)).

➤ **To view Ethernet port information:**

- Open the Ethernet Port Information page (**Status & Diagnostics** tab > **System Status** menu > **Ethernet Port Information**).

	Active	Speed	Duplex Mode	Power Over Ethernet Status	Power Over Ethernet Allocated Power
1	Yes	1000 Mbps	Full Duplex	Invalid signature	N/A
2	No	10 Mbps	Half Duplex	Enabled	N/A
3	No	10 Mbps	Half Duplex	Enabled	N/A
4	No	10 Mbps	Half Duplex	Enabled	N/A
5	No	10 Mbps	Half Duplex	Enabled	N/A
6	No	10 Mbps	Half Duplex	Enabled	N/A
7	No	10 Mbps	Half Duplex	Enabled	N/A
8	No	10 Mbps	Half Duplex	Enabled	N/A
9	No	10 Mbps	Half Duplex	Enabled	N/A
10	No	10 Mbps	Half Duplex	Enabled	N/A
11	No	10 Mbps	Half Duplex	Enabled	N/A
12	No	10 Mbps	Half Duplex	Enabled	N/A

▼ System Power Information	
Power Budget	120000 [mWatt]
Allocated Power	0 [mWatt]
Remaining Power	120000 [mWatt]

### Ethernet Port Information Parameters

Parameter	Description
Active	Displays whether the port is active or not.
Speed	Displays the speed (in Mbps) of the Ethernet port.
Duplex Mode	Displays whether the port is half- or full-duplex.
State	Displays the state of the port: <ul style="list-style-type: none"> <li>▪ "Forwarding": Active port (data is being received and sent)</li> <li>▪ "Disabled": Redundancy port</li> </ul>
Power Over Ethernet Status	Displays whether Power over Ethernet (PoE) is active on the port.
Power Over Ethernet Allocated Power	Displays the power allocated to the port.
Power Budget	Displays the power budget.
Allocated Power	Displays the power allocated to the ports.
Remaining Power	Displays the power available for additional ports.

## 48 Carrier-Grade Alarms

This section describes how to view the following types of alarms:

- Active alarms - see 'Viewing Active Alarms' on page 579
- Alarm history - see 'Viewing Alarm History' on page 579

### 48.1 Viewing Active Alarms

The Active Alarms page displays a list of currently active alarms. You can also access this page from the Home page (see 'Viewing the Home Page' on page 54).

➤ To view the list of active alarms:

- Open the Active Alarms page (**Status & Diagnostics** tab > **System Status** menu > **Carrier-Grade Alarms** > **Active Alarms**).

Sequential number	Severity	Source	Description	Date
3	Major	Board#1/WanLink#1	WAN link alarm. FE interface 1 is down.	23.2.2010 , 2:13:31
4	Minor	Board#1/EthernetLink#2	Ethernet link alarm. LAN port number 2 is down.	23.2.2010 , 2:13:31
5	Minor	Board#1/EthernetLink#3	Ethernet link alarm. LAN port number 3 is down.	23.2.2010 , 2:13:31
6	Minor	Board#1/EthernetLink#4	Ethernet link alarm. LAN port number 4 is down.	23.2.2010 , 2:13:31
7	Minor	Board#1/EthernetLink#5	Ethernet link alarm. LAN port number 5 is down.	23.2.2010 , 2:13:31
8	Minor	Board#1/EthernetLink#6	Ethernet link alarm. LAN port number 6 is down.	23.2.2010 , 2:13:31
9	Minor	Board#1/EthernetLink#7	Ethernet link alarm. LAN port number 7 is down.	23.2.2010 , 2:13:31
10	Minor	Board#1/EthernetLink#8	Ethernet link alarm. LAN port number 8 is down.	23.2.2010 , 2:13:31
11	Minor	Board#1/EthernetLink#9	Ethernet link alarm. LAN port number 9 is down.	23.2.2010 , 2:13:31
12	Minor	Board#1/EthernetLink#10	Ethernet link alarm. LAN port number 10 is down.	23.2.2010 , 2:13:31
13	Minor	Board#1/EthernetLink#11	Ethernet link alarm. LAN port number 11 is down.	23.2.2010 , 2:13:31
14	Minor	Board#1/EthernetLink#12	Ethernet link alarm. LAN port number 12 is down.	23.2.2010 , 2:13:31

For each alarm, the following information is provided:

- **Severity:** severity level of the alarm:
  - Critical (red)
  - Major (orange)
  - Minor (yellow)
- **Source:** unit from which the alarm was raised
- **Description:** brief explanation of the alarm
- **Date:** date and time that the alarm was generated

You can view the next 20 alarms (if exist), by clicking the **Go to page** button.

### 48.2 Viewing Alarm History

The Alarms History page displays a list of alarms that have been raised and traps that have been cleared.

➤ To view the list of history alarms:

- Open the Alarms History page (**Status & Diagnostics** tab > **System Status** menu > **Carrier-Grade Alarms** > **Alarms History**).

Sequential number	Severity	Source	Description	Date
1	Major	Board#1	Controller failure alarm Proxy Set 0: Proxy lost. looking for another proxy	6.1.2010 , 14:1:26
2	cleared	Board#1	Alarm cleared: Controller failure alarm Proxy Set 0: Proxy lost. looking for another proxy	6.1.2010 , 14:1:26
3	Major	Board#1	Controller failure alarm Proxy Set ID 0	6.1.2010 , 14:1:26
4	Major	Board#1/WanLink#1	WAN link alarm. FE interface 1 is down.	6.1.2010 , 14:1:29
5	Minor	Board#1/EthernetLink#2	Ethernet link alarm. LAN port number 2 is down.	6.1.2010 , 14:1:29
6	Major	Board#1	NTP server alarm. No connection to NTP server.	6.1.2010 , 14:11:14

For each alarm, the following information is provided:

- **Severity:** severity level of the alarm:
  - Critical (red)
  - Major (range)
  - Minor (yellow)
  - Cleared (green)
- **Source:** unit from which the alarm was raised
- **Description:** brief explanation of the alarm
- **Date:** date and time that the alarm was generated

To view the next 20 alarms (if exist), click the **Go to page** button.

➤ **To delete all the alarms in the table:**

1. Click the **Delete History Table** button; a confirmation message box appears.
2. Click **OK** to confirm.



## 49 Performance Monitoring

This section describes how to view performance monitoring.

### 49.1 Viewing MOS per Media Realm

The MOS Per Media Realm page displays statistics on Media Realms (configured in 'Configuring Media Realms' on page 168). This page provides two graphs:

- Upper graph: displays the Mean Opinion Score (MOS) quality in RTCP data per selected Media Realm.
- Lower graph: displays the bandwidth of transmitted media (in Kbps) in RTCP data per Media Realm.



➤ **To view the MOS per Media Realm graph:**

1. Open the MOS Per Media Realm page (**Status & Diagnostics** tab > **Performance Monitoring** menu > **MOS Per Media Realm**).

**Figure 49-1: MOS Per Media Realm Graph**



2. From the 'Media Realm' drop-down list, select the Media Realm for which you want to view.

Use the **Zoom In**  button to increase the displayed time resolution or the **Zoom Out**  button to decrease it. Instead of using these zoom buttons, you can use the slide ruler. As you increase the resolution, more data is displayed on the graph. The minimum resolution is about 30 seconds; the maximum resolution is about an hour.

To pause the graph, click the **Pause** button; click **Play** to resume.

## 49.2 Viewing Trunk Utilization

The Trunk Utilization page provides an X-Y graph that displays the number of active channels per trunk over time. The x-axis indicates the time; the y-axis indicates the number of active trunk channels.



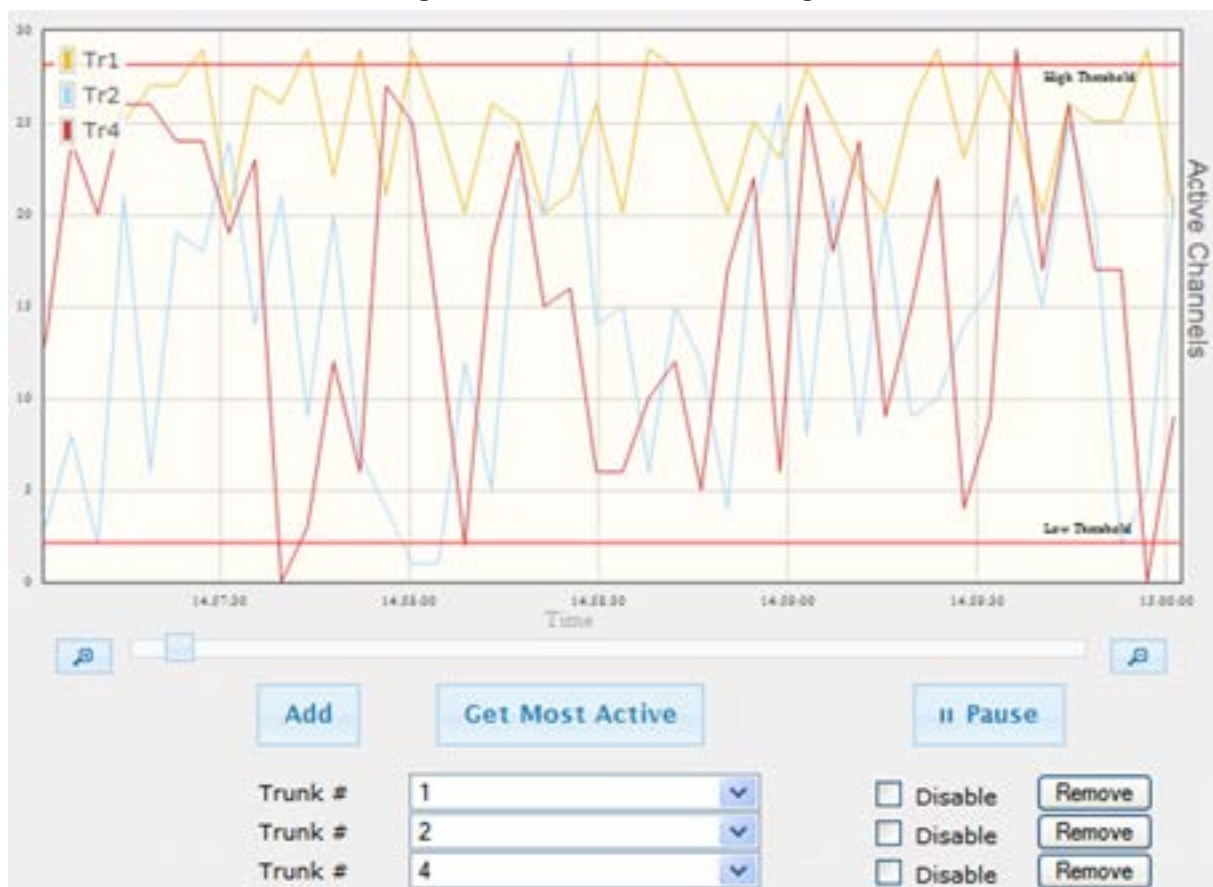
### Notes:

- This page is available only if you have trunks and the SBC application is disabled.
- If you navigate to a different page, the data displayed in the graph and all its settings are cleared.

### ➤ To view the number of active trunk channels

1. Open the Trunk Utilization page (**Status & Diagnostics** tab > **Performance Monitoring** menu > **Trunk Utilization**).



Figure 49-2: Trunk Utilization Page



2. From the 'Trunk' drop-down list, select the trunk for which you want to view active channels.

For more graph functionality, see the following table:

**Additional Graph Functionality for Trunk Utilization**

Button	Description
<b>Add</b> button	Displays additional trunks in the graph. Up to five trunks can be displayed simultaneously in the graph. To view another trunk, click this button and then from the new 'Trunk' drop-down list, select the required trunk.  Each trunk is displayed in a different color, according to the legend shown in the top-left corner of the graph.
<b>Remove</b> button	Removes the selected trunk display from the graph.
<b>Disable</b> check box	Hides or shows an already selected trunk. Select this check box to temporarily hide the trunk display; clear this check box to show the trunk. This is useful if you do not want to remove the trunk entirely (using the <b>Remove</b> button).
<b>Get Most Active</b> button	Displays only the trunk with the most active channels (i.e., trunk with the most calls).
<b>Pause</b> button	Pauses the display in the graph.
<b>Play</b> button	Resumes the display in the graph.
<b>Zoom</b> slide ruler and buttons	Increases or reduces the trunk utilization display resolution concerning time. The <b>Zoom In</b>  button increases the time resolution; the <b>Zoom Out</b>  button decreases it. Instead of using the 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.

## 49.3 Viewing Quality of Experience

The Quality Of Experience page provides statistical information on calls per SRD or IP Group. The statistics can be further filtered to display incoming and/or outgoing call direction, and type of SIP dialog (INVITE, SUBSCRIBE, or all).



**Note:** This page is available only if the SBC application has been enabled.

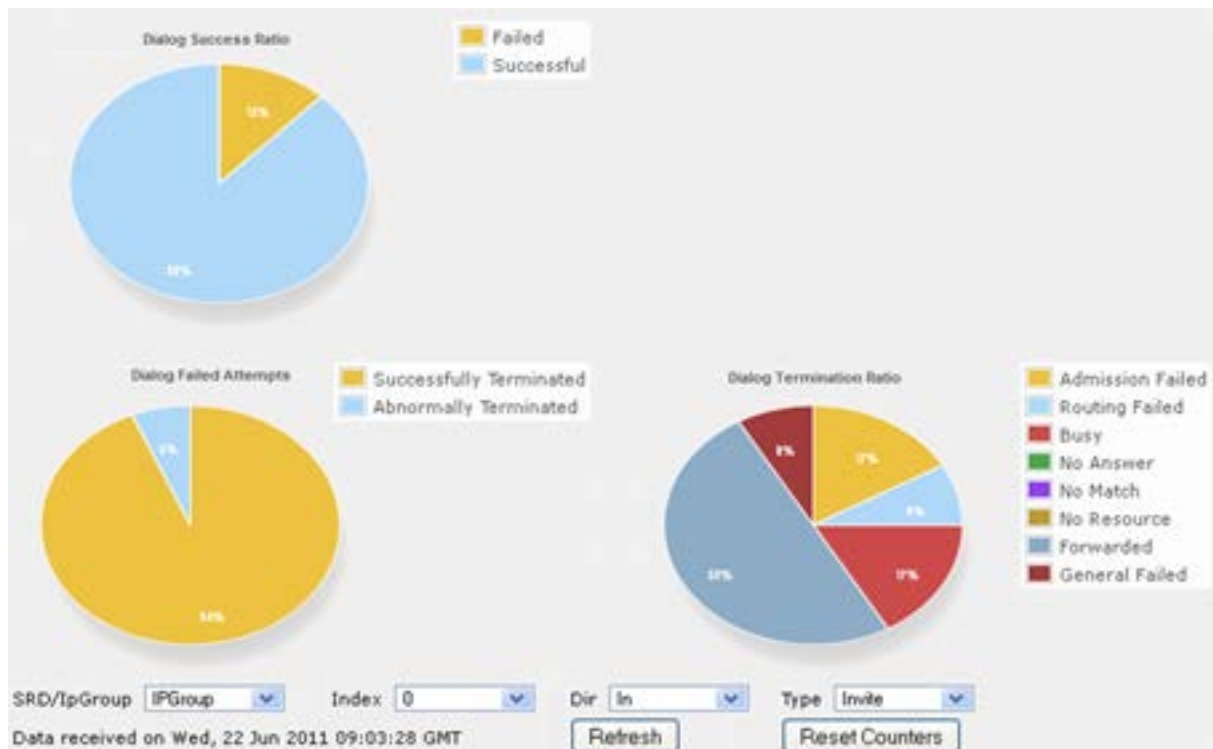
This page provides three pie charts:

- Dialog Success Ratio: displays the SIP call and subscribe (SUBSCRIBE) dialog success-failed ratio.
- Dialog Failed Attempts: displays the failed call attempts. This includes the number of calls and subscribes which were successfully and abnormally terminated.
- Dialog Termination Ratio: displays call termination by reason (e.g., due to no answer).

➤ **To view Quality of Experience:**

1. Open the Quality Of Experience page (**Status & Diagnostics** tab > **Performance Monitoring** menu > **Quality Of Experience**).

**Figure 49-3: Quality Of Experience Graph**



2. From the 'SRD/IpGroup' drop-down list, select whether you want to view QoE for an SRD or IP Group.
3. From the 'Index' drop-down list, select the SRD or IP Group index.
4. From the 'Dir' drop-down list, select the call direction:
  - **In** - incoming calls
  - **Out** - outgoing calls
  - **Both** - incoming and outgoing calls
5. From the 'Type' drop-down list, select the SIP message type:
  - **Invite** - INVITE
  - **Subscribe** - SUBSCRIBE
  - **Other** - all SIP messages

To refresh the charts, click **Refresh**. To reset the counters, click **Reset Counters**.

## 49.4 Viewing Average Call Duration

The Average Call Duration page displays information about a specific SRD or IP Group. This page includes two graphs:

- Upper graph: displays the number of calls (INVITEs).
- Lower graph: displays the average call duration.



**Note:** This page is available only if the SBC application has been enabled.



➤ **To view average call duration:**

1. Open the Average Call Duration page (**Status & Diagnostics** tab > **Performance Monitoring** menu > **Average Call Duration**).

**Figure 49-4: Average Call Duration Graph**



2. From the 'SRD/IpGroup' drop-down list, select whether you want to view information for an SRD or IP Group.
3. From the 'Index' drop-down list, select the SRD or IP Group index.

Use the **Zoom In**  button to increase the displayed time resolution or the **Zoom Out**  button to decrease it. Instead of using these zoom buttons, you can use the slide ruler. As you increase the resolution, more data is displayed on the graph. The minimum resolution is about 30 seconds; the maximum resolution is about an hour.

To pause the graph, click the **Pause** button; click **Play** to resume.

## 49.5 Network Monitoring (Probing) Two Devices

The device can be configured to monitor the quality of the network path (network quality monitoring - NQM) between it and other AudioCodes devices. The path monitoring is done by sending packets from a "sender" device to a "responder" device and then calculating the round-trip time (RTT), packet loss (PL), and jitter. Since both responder and sender nodes are AudioCodes devices, the monitoring is done by sending RTP/RTCP packets in a way

that accurately predicts the WAN service-level agreement (SLA) granted for real VoIP calls by the network.

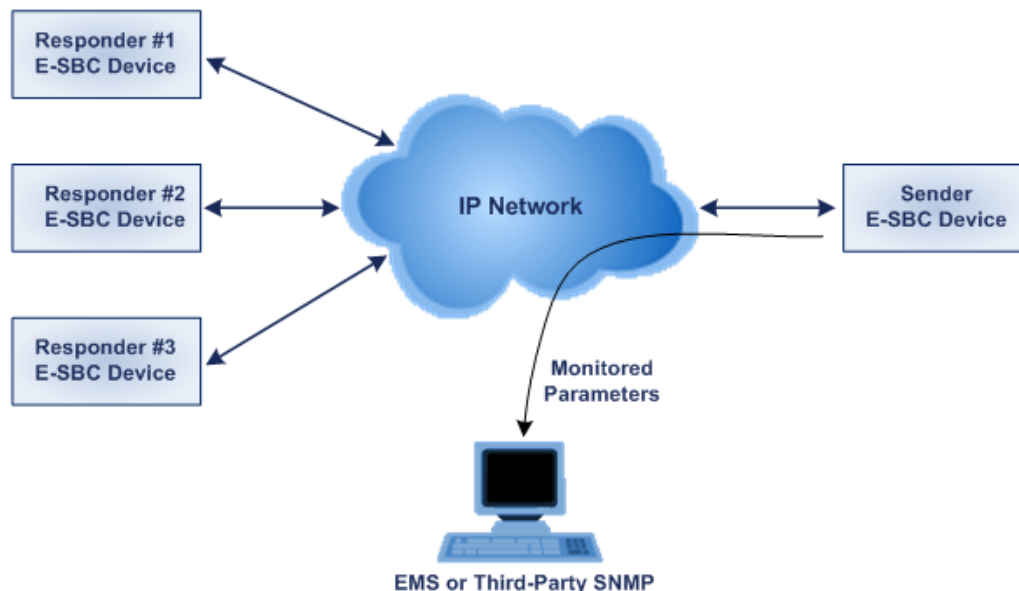


**Note:** If the packets sent mimic a G.711 or G.729 stream, the following quality measurements are also done:

- Listener quality MOS per ITU-T specification
- Conversation quality MOS per ITU-T specification

You can configure up to 10 network quality probing paths. For example, you can configure three probing paths, where your device is configured as a sender for three different responder devices, as shown in the figure below:

**Figure 49-5: Network Quality Probing Example**



You can periodically poll the device for the latest VoIP quality metrics and specify thresholds for the quality metrics mentioned above. If these thresholds are crossed, the device generates the following SNMP traps to Audiocodes EMS or third-party SNMP-based manager:

- NqmConnectivityAlarm: Connectivity with monitored probe destination is lost
- NqmRttAlarm: High RTP detected toward probe destination
- NqmJitterAlarm: High jitter detected toward probe destination
- NqmPacketLossAlarm: High packet loss detected toward probe destination

This feature is configured using the CLI. Below is a list of some of the CLI commands. For a full list and description of the related CLI commands, refer to the *MSBR Series CLI Reference Guide for System and VoIP Functionalities*.

- nqm responder-table – adds a responder (IP address and port)
- nqm probing-table – defines the polling attributes (duration and frequency)
- nqm sender-table - adds a sender (including RTT, PL, and jitter thresholds; associates probing definition; responder address; local interface)

The following procedure describes how to quickly configure network quality probing.

➤ **To configure network quality probing:**

1. Configure the "sender termination" side:

a. Bind a WAN interface to the NQM service:

```
(config-system) bind GigabitEthernet 0/0 nqm
```



**Note:** The chosen WAN interface should be the interface on which the NQM packets are planned to flow bi-directionally and binding is necessary to create the corresponding static NAT rules. If the NQM session is planned to flow within the LAN then no binding is needed and this step can be skipped.

b. Configure a row in the Probing table:

```
(config-system)# nqm probing-table 0
(probing-table-0)# set probe-name voip_probe_1 ;
identifies this line
(probing-table-0)# set start-time now ; starting time of
this probe
(probing-table-0)# exit ; activates the probe
```

c. Configure a row in the Sender table to define a sender termination:

```
(config-system)# nqm sender-table 0
(sender-table-0)# set sender-name
main_office_voip_checker_1 ; identifies specific sender
(sender-table-0)# set target-ip 10.4.3.98 ; IP address
of responder termination
(sender-table-0)# set target-port 3900 ; listening port
number at responder termination
```



**Note:** A responder termination defined by the pair <target IP address, target port> can be defined only once for a single sender line; multiple senders can't be defined to send packets to the same responder termination.

```
(sender-table-0)# set probe-name voip_probe_1 ; name
of probing row previously configured to be used by this
sender
```



**Note:** A single row in the Probing table may be shared by several senders, thereby sharing and simplifying common attributes.

```
(sender-table-0)# set source-interface-name NQM_WAN ;
name of network interface to send packets from
```



**Note:** If you want to output packets to the WAN interface, simply set NQM\_WAN as the source interface name; otherwise, set the interface name to a specific interface name listed in the network interface table.

```
(sender-table-0)# exit ; activates the sender line
```



2. Configure the "responder termination" side:

a. Bind a WAN interface to the NQM service:

```
(config-system) bind GigabitEthernet 0/0 nqm
```



**Note:** The chosen WAN interface should be the interface on which the NQM packets are planned to flow bi-directionally and binding is necessary to create the corresponding static NAT rules. If the NQM session is planned to flow within the LAN then no binding is needed and this step can be skipped.

b. Configure a row in the Responder table:

```
(config-system)# nqm responder-table 0
(responder-table-0)# set responder-name
vmain_office_voip_responder_1 ; name tag to identify
this line
(responder-table-0)# set local-port 3900 ; listening
port number at responder termination
(responder-table-0)# exit ; activates the probe line
```



**Note:** Ensure that the local-port value is the same as the target-port value set for the corresponding sender termination.

```
(responder-table-0)# set source-interface-name NQM_WAN ;
name of network interface to send packets from
```



**Notes:**

- If you want to listen to the WAN interface, simply set NQM\_WAN as the source interface name; otherwise, set the interface name to a specific interface name listed in the network interface table.
- Ensure that the network interface the responder termination is listening upon is in-sync with the target-ip value set for the corresponding sender termination.

```
(responder-table-0)# exit ; activates the responder line
```

➤ To view NQM results:

- On the sender termination device, type the following command to view eight result rows of sender "0":

```
# show system nqm 0 8
```

Figure 49-6: Example of NQM Results

Probe Time	Valid	RTT	PL Tx	PL Rx	Total PL	Jit. Tx	Jit. Rx	Total Jit.	MOS CQ	MOS LQ
01-01-2010@02:46:24	yes	7	0	0	0	0	17	17	0.0	0.0
01-01-2010@02:47:24	yes	10	0	0	0	30	1	31	0.0	0.0
01-01-2010@02:48:25	yes	9	0	0	0	31	20	51	0.0	0.0
01-01-2010@02:49:25	yes	6	0	0	0	32	4	36	0.0	0.0
01-01-2010@02:50:25	yes	5	0	0	0	0	5	5	0.0	0.0
01-01-2010@02:51:25	yes	5	0	0	0	15	15	30	0.0	0.0
01-01-2010@02:52:25	yes	6	0	0	0	32	7	39	0.0	0.0
01-01-2010@02:53:25	yes	6	0	0	0	30	5	35	0.0	0.0



## 50 VoIP Status

This section describes how to view VoIP status and statistics.


































## 50.1 Viewing Trunks & Channels Status

The Trunks & Channels Status page displays the status of the device's trunks and corresponding channels. It also enables you to view trunk configuration and channel information.

➤ **To view the status of the device's trunks and channels:**

1. Open the Home page.
2. On the graphical display of the device, click the required trunk, and then from the shortcut menu, choose Port Settings; the Trunks & Channels Status page appears.

### Figure 50-1: Trunks and Channels Status Screen

Trunks		Channels																															
Status	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
 Trunk 1																																	



**Note:** The number of displayed trunks and channels depends on configuration.









The status of the trunks is depicted by color-coded icons, as described in the table below:

### Description of Color-Coded Icons for Trunk Status

Icon	Color	Trunk
		Label
	Gray	<b>Disabled</b>
	Green	<b>Active - OK</b>
	Yellow	<b>RAI Alarm</b>
	Red	<b>LOS / LOF Alarm</b>
	Blue	<b>AIS Alarm</b>
	Light Orange	<b>D-Channel Alarm</b>
	Dark Orange	<b>NFAS Alarm</b>
	Purple	<b>Lower Layer Down (DS3 physical layer is disabled)</b>





The status of the channels is depicted by color-coded icons, as described in the table below:

**Description of Color-Coded Icons for Channel Status**

Icon	Color	Label	Description
	Light blue	<b>Inactive</b>	Channel is configured, but currently has no calls
	Green	<b>Active</b>	Call in progress (RTP traffic) and no alarms
	Purple	<b>SS7</b>	Channel is configured for SS7 <b>Note:</b> Currently, SS7 is not supported.
	Gray	<b>Non Voice</b>	Channel is not configured
	Blue	<b>ISDN Signaling</b>	Channel is configured as a D-channel
	Yellow	<b>CAS Blocked</b>	-
	Dark Orange	<b>Maintenance</b>	B-channel has been intentionally taken out of service due to maintenance
	Red	<b>Out Of Service</b>	B-channel is out of service

- To view detailed information on a specific trunk's channel, click the required channel icon; the Basic Channel Information page [appears](#), displaying information under the **Basic** tab (displayed in green):

**Figure 50-2: Basic Channel Information Page**

 SIP  <b>Basic</b>  RTP/RTCP  Voice Settings	
Channel Identifier:	55
Status:	Inactive
Call ID:	0
Endpoint ID:	Not Available
Call Duration [sec]:	0
Call Type:	Voice
Call Destination:	10.13.4.12
Coder:	Transparent

To view additional channel information, click the required tab (**SIP**, **RTP/RTCP**, and **Voice Settings**).

- To view the settings of a specific trunk, click the required trunk icon, and then from the shortcut menu, choose **Port Settings**; the Trunk Settings page opens, displaying the trunk's settings. If needed, you can modify the settings (see 'Configuring Trunk Settings' on page [271](#)).

## 50.2 Viewing Analog Port Information

The Home page allows you to view detailed information on selected FXS and FXO analog ports such as RTP/RTCP and voice settings.

### ➤ To view information on an analog port:

- Open the Home page.
- On the graphical display of the device, click the required analog port; a shortcut menu

appears.

3. From the shortcut menu, choose **Port Settings**; the Basic Channel Information page appears with the **Basic** tab selected (displayed in green):

**Figure 50-3: Basic Channel Information Page**

◆ SIP ◆ Basic ◆ RTP/RTCP ◆ Voice Settings	
Channel Identifier:	55
Status:	Inactive
Call ID:	0
Endpoint ID:	Not Available
Call Duration [sec]:	0
Call Type:	Voice
Call Destination:	10.13.4.12
Coder:	Transparent

4. To view additional channel information, click the required tab - **SIP**, **RTP/RTCP**, and **Voice Settings**.

## 50.3 Viewing NFAS Groups and D-Channel Status

The NFAS Group & D-Channel Status page displays the status of the device's D-channels and NFAS groups. The status of a D-channel and NFAS group can be "In Service" or "Out of Service". This page also indicates whether the D-channel is a primary or backup D-channel.

This page also enables you to manually switchover between active and standby D-channels belonging to the same NFAS group. This is done using the **Switch Activity** button. For more information, see 'Performing Manual D-Channel Switchover in NFAS Group' on page 286.



**Note:** This page is applicable only to T1 ISDN protocols supporting NFAS, and only if the NFAS group is configured with two D-channels.

- To view the status of the D-channels and NFAS groups:

- Open the NFAS Group & D-Channel Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **NFAS Group & D-Channel Status**).

**Figure 50-4: NFAS Group & D-Channel Status Page**

▼ NFAS Group #2

Status: **In Service**  
D-Channels:

Trunk#1  
Configuration: Primary  
Status: **In Service**  
NFAS Status: Active

Trunk#2  
Configuration: Backup  
Status: **Out Of Service**  
NFAS Status: Not Applicable

Switch Activity Group #2

## 50.4 Viewing Active IP Interfaces

The IP Interface Status page displays the device's active IP interfaces that are listed in the Multiple Interface Table page (see 'Configuring IP Network Interfaces' on page 107).

➤ **To view the active IP network interfaces:**

- Open the IP Interface Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **IP Interface Status**).

Index	Application Type	Address Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	O+M+C	IPv4	IPv4 Manual	10.13.4.12	16	10.13.0.1	1	Voice
NA	Internal	IPv4	IPv4 Manual	169.254.254.254	30	169.254.254.253	4001	InternalIF

## 50.5 Viewing Performance Statistics

The Basic Statistics page provides read-only, device performance statistics. This page is refreshed every 60 seconds. The duration that the currently displayed statistics has been collected is displayed above the statistics table.

➤ **To view performance statistics:**

- Open the Basic Statistics page (**Status & Diagnostics** tab > **VoIP Status** menu > **Performance Statistics**).

**Figure 50-5: Basic Statistics Page**

(Statistics for 759525 seconds)	
Active TDM channels	0
Active DSP resources	0
Active analog channels	0
Active G.711 channels	0
Average voice delay (ms)	5
Average voice jitter (ms)	11
Total RTP packets TX	4250
Total RTP packets RX	4241
Total call attempts	6

The duration that the displayed statistics were collected is displayed in seconds above the table. To reset the performance statistics to zero, click the **Reset Statistics** button.

## 50.6 Viewing Call Counters

The IP to Tel Calls Count page and Tel to IP Calls Count page provide you with statistical information on incoming (IP-to-Tel) and outgoing (Tel-to-IP) calls. The statistical information is updated according to the release reason that is received after a call is terminated (during the same time as the end-of-call Call Detail Record or CDR message is sent). The release reason can be viewed in the 'Termination Reason' field in the CDR message.

You can reset the statistical data displayed on the page (i.e., refresh the display), by clicking the **Reset Counters** button located below the table.

➤ **To view IP-to-Tel and Tel-to-IP call counters:**

- Open the Call Counters page that you want to view (**Status & Diagnostics** tab > **VoIP Status** menu > **IP to Tel Calls Count** or **Tel to IP Calls Count**); the figure below shows the IP to Tel Calls Count page.

**Figure 50-6: Calls Count Page**

▼	
Number of Attempted Calls	19
Number of Established Calls	14
Percentage of Successful Calls(ASR)	73.684211
Number of Calls Terminated due to a Busy Line	2
Number of Calls Terminated due to No Answer	0
Number of Calls Terminated due to Forward	0
Number of Failed Calls due to No Route	0
Number of Failed Calls due to No Matched Capabilities	0
Number of Failed Calls due to No Resources	0
Number of Failed Calls due to Other Failures	0
Average Call Duration(ACD)[sec]	25
Attempted Fax Calls Counter	0
Successful Fax Calls Counter	0

The fields in this page are described in the following table:

**Call Counters Description**

Counter	Description
<b>Number of Attempted Calls</b>	Indicates the number of attempted calls. It is composed of established and failed calls. The number of established calls is represented by the 'Number of Established Calls' counter. The number of failed calls is represented by the failed-call counters. Only one of the established / failed call counters is incremented every time.
<b>Number of Established Calls</b>	Indicates the number of established calls. It is incremented as a result of one of the following release reasons if the duration of the call is greater than zero: <ul style="list-style-type: none"> <li>GWAPP_REASON_NOT_RELEVANT (0)</li> <li>GWAPP_NORMAL_CALL_CLEAR (16)</li> <li>GWAPP_NORMAL_UNSPECIFIED (31)</li> </ul> And the internal reasons: <ul style="list-style-type: none"> <li>RELEASE_BECAUSE_UNKNOWN_REASON</li> <li>RELEASE_BECAUSE_REMOTE_CANCEL_CALL</li> <li>RELEASE_BECAUSE_MANUAL_DISC</li> <li>RELEASE_BECAUSE_SILENCE_DISC</li> <li>RELEASE_BECAUSE_DISCONNECT_CODE</li> </ul> <b>Note:</b> When the duration of the call is zero, the release reason GWAPP_NORMAL_CALL_CLEAR increments the 'Number of Failed Calls due to No Answer' counter. The rest of the release reasons increment the 'Number of Failed Calls due to Other Failures' counter.
<b>Percentage of Successful Calls (ASR)</b>	The percentage of established calls from attempted calls.
<b>Number of Calls Terminated due to a Busy Line</b>	Indicates the number of calls that failed as a result of a busy line. It is incremented as a result of the following release reason: GWAPP_USER_BUSY (17)

Counter	Description
<b>Number of Calls Terminated due to No Answer</b>	Indicates the number of calls that weren't answered. It's incremented as a result of one of the following release reasons: <ul style="list-style-type: none"> <li>GWAPP_NO_USER_RESPONDING (18)</li> <li>GWAPP_NO_ANSWER_FROM_USER_ALERTED (19)</li> <li>GWAPP_NORMAL_CALL_CLEAR (16) (when the call duration is zero)</li> </ul>
<b>Number of Calls Terminated due to Forward</b>	Indicates the number of calls that were terminated due to a call forward. The counter is incremented as a result of the following release reason: RELEASE_BECAUSE_FORWARD
<b>Number of Failed Calls due to No Route</b>	Indicates the number of calls whose destinations weren't found. It is incremented as a result of one of the following release reasons: <ul style="list-style-type: none"> <li>GWAPP_UNASSIGNED_NUMBER (1)</li> <li>GWAPP_NO_ROUTE_TO_DESTINATION (3)</li> </ul>
<b>Number of Failed Calls due to No Matched Capabilities</b>	Indicates the number of calls that failed due to mismatched device capabilities. It is incremented as a result of an internal identification of capability mismatch. This mismatch is reflected to CDR via the value of the parameter DefaultReleaseReason (default is GWAPP_NO_ROUTE_TO_DESTINATION (3)) or by the GWAPP_SERVICE_NOT_IMPLEMENTED_UNSPECIFIED (79) reason.
<b>Number of Failed Calls due to No Resources</b>	Indicates the number of calls that failed due to unavailable resources or a device lock. The counter is incremented as a result of one of the following release reasons: <ul style="list-style-type: none"> <li>GWAPP_RESOURCE_UNAVAILABLE_UNSPECIFIED</li> <li>RELEASE_BECAUSE_GW_LOCKED</li> </ul>
<b>Number of Failed Calls due to Other Failures</b>	This counter is incremented as a result of calls that failed due to reasons not covered by the other counters.
<b>Average Call Duration (ACD) [sec]</b>	The average call duration (ACD) in seconds of established calls. The ACD value is refreshed every 15 minutes and therefore, this value reflects the average duration of all established calls made within a 15 minute period.
<b>Attempted Fax Calls Counter</b>	Indicates the number of attempted fax calls.
<b>Successful Fax Calls Counter</b>	Indicates the number of successful fax calls.

## 50.7 Viewing Registered Users

The SAS/SBC Registered Users page displays a list of registered SAS/SBC users recorded in the device's database.

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

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

Figure 50-7: SAS/SBC Registered Users Page

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

SAS/SBC Registered Users Parameters

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

## 50.8 Viewing Registration Status

The Registration Status page displays whether the device as a whole, its endpoints (FXS / FXO / BRI), and SIP Accounts are registered to a SIP Registrar/Proxy server.

➤ **To view the registration status:**

- Open the Registration Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **Registration Status**).

Registered Per Gateway				NO
▼ Ports Registration Status				
Gateway Port				Status
Module	3 Port	1 FXS	NOT REGISTERED	
Module	3 Port	2 FXS	NOT REGISTERED	
Module	3 Port	3 FXS	NOT REGISTERED	
Module	3 Port	4 FXS	NOT REGISTERED	
▼ Accounts Registration Status				
Index	Group Type		Group Name	Status
▼ BRI Phone Numbers Status				
Phone Number		Module / Port		Status

- **Registered Per Gateway:**
  - "YES" = Registration is per device
  - "NO" = Registration is not per device
- **Ports Registration Status:**
  - "REGISTERED" = channel is registered
  - "NOT REGISTERED" = channel not registered

- **Accounts Registration Status:** registration status based on the Accounts table (configured in 'Configuring Account Table' on page 219):
  - **Group Type:** type of served group - Trunk Group or IP Group
  - **Group Name:** name of the served group, if applicable
  - **Status:** indicates whether or not the group is registered ("Registered" or "Unregistered")
- **BRI Phone Number Status:**
  - **Phone Number:** phone number of BRI endpoint
  - **Module/Port:** module/port number of BRI endpoint
  - **Status:** indicates whether or not the BRI endpoint is registered ("Registered" or "Unregistered")



**Note:** The registration mode (i.e., per device, endpoint, account. or no registration) is configured in the Hunt Group Settings table (see 'Configuring Hunt Group Settings' on page 291) or using the TrunkGroupSettings *ini* file parameter.

## 50.9 Viewing Call Routing Status

The Call Routing Status page provides you with information on the current routing method used by the device. This information includes the IP address and FQDN (if used) of the Proxy server with which the device currently operates.

➤ **To view call routing status:**

- Open the Call Routing Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **Call Routing Status**).

**Figure 50-8: Call Routing Status Page**

Call-Routing Method			Routing Table		
▼ Active Proxy Sets Status					
ID	IP Address			State	
0	Not Used (--)			--	
1	10.8.230.64 (10.8.230.64)			OK	
2	10.9.244.80 (10.9.244.80)			OK	
3	10.10.244.80 (10.10.244.80)			OK	
4	10.11.244.80 (10.11.244.80)			OK	
5	10.12.244.80 (10.12.244.80)			OK	
6	Not Used (--)			--	
7	Not Used (--)			--	
8	Not Used (--)			--	
9	10.8.244.81 (10.8.244.81)			OK	
10	Not Used (--)			--	
11	Not Used (--)			--	
12	Not Used (--)			--	

**Call Routing Status Parameters**

Parameter	Description
<b>Call-Routing Method</b>	<ul style="list-style-type: none"> <li>▪ Proxy/GK = Proxy server is used to route calls.</li> <li>▪ Routing Table = Outbound IP Routing table is used to route calls.</li> </ul>
<b>IP Address</b>	<ul style="list-style-type: none"> <li>▪ Not Used = Proxy server isn't defined.</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>IP address and FQDN (if exists) of the Proxy server with which the device currently operates.</li> </ul>
<b>State</b>	<ul style="list-style-type: none"> <li>N/A = Proxy server isn't defined.</li> <li>OK = Communication with the Proxy server is in order.</li> <li>Fail = No response from any of the defined Proxies.</li> </ul>

## 50.10 Viewing IP Connectivity

The IP Connectivity page displays on-line, read-only network diagnostic connectivity information on all destination IP addresses configured in the Outbound IP Routing Table page (see 'Configuring Outbound IP Routing Table' on page 321).



**Note:** The information in columns 'Quality Status' and 'Quality Info' (per IP address) is reset if two minutes elapse without a call to that destination.

➤ **To view IP connectivity information:**

1. In the Routing General Parameters page, set the 'Enable Alt Routing Tel to IP' parameter (AltRoutingTel2IPMode) to **Enable** or **Status Only** (see 'Configuring General Routing Parameters' on page 321).
2. Open the IP Connectivity page (**Status & Diagnostics** tab > **VoIP Status** menu > **IP Connectivity**).

**Figure 50-9: IP Connectivity Page**

	IP Address	Host Name	Connectivity Method	Connectivity Status	Quality Status	Quality Info	DNS Status
1	Unused	---	Ping	---	---	---	---
2	Unused	---	Ping	---	---	---	---
3	Unused	---	Ping	---	---	---	---
4	Unused	---	Ping	---	---	---	---
5	Unused	---	Ping	---	---	---	---
6	Unused	---	Ping	---	---	---	---
7	Unused	---	Ping	---	---	---	---
8	Unused	---	Ping	---	---	---	---
9	Unused	---	Ping	---	---	---	---
10	Unused	---	Ping	---	---	---	---
11	Unused	---	Ping	---	---	---	---
12	Unused	---	Ping	---	---	---	---

**IP Connectivity Parameters**

Column Name	Description
<b>IP Address</b>	<p>The IP address can be one of the following:</p> <ul style="list-style-type: none"> <li>IP address defined as the destination IP address in the Outbound IP Routing Table.</li> </ul>

Column Name	Description
	<ul style="list-style-type: none"> <li>IP address resolved from the host name defined as the destination IP address in the Outbound IP Routing Table.</li> </ul>
<b>Host Name</b>	Host name (or IP address) as defined in the Outbound IP Routing Table.
<b>Connectivity Method</b>	The method according to which the destination IP address is queried periodically (SIP OPTIONS request).
<b>Connectivity Status</b>	<p>The status of the IP address' connectivity according to the method in the 'Connectivity Method' field.</p> <ul style="list-style-type: none"> <li>OK = Remote side responds to periodic connectivity queries.</li> <li>Lost = Remote side didn't respond for a short period.</li> <li>Fail = Remote side doesn't respond.</li> <li>Init = Connectivity queries not started (e.g., IP address not resolved).</li> <li>Disable = The connectivity option is disabled, i.e., parameter 'Alt Routing Tel to IP Mode' (AltRoutingTel2IPMode <i>in</i>) is set to 'None' or 'QoS'.</li> </ul>
<b>Quality Status</b>	<p>Determines the QoS (according to packet loss and delay) of the IP address.</p> <ul style="list-style-type: none"> <li>Unknown = Recent quality information isn't available.</li> <li>OK</li> <li>Poor</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only if the parameter 'Alt Routing Tel to IP Mode' is set to 'QoS' or 'Both' (AltRoutingTel2IPMode = 2 or 3).</li> <li>This parameter is reset if no QoS information is received for 2 minutes.</li> </ul>
<b>Quality Info.</b>	<p>Displays QoS information: delay and packet loss, calculated according to previous calls.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only if the parameter 'Alt Routing Tel to IP Mode' is set to 'QoS' or 'Both' (AltRoutingTel2IPMode = 2 or 3).</li> <li>This parameter is reset if no QoS information is received for 2 minutes.</li> </ul>
<b>DNS Status</b>	<p>DNS status can be one of the following:</p> <ul style="list-style-type: none"> <li>DNS Disable</li> <li>DNS Resolved</li> <li>DNS Unresolved</li> </ul>

## 51 Data Status

This section describes how to view data-touter status and statistics.

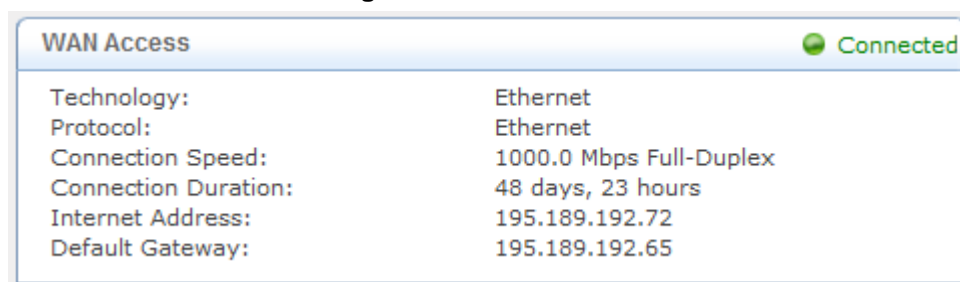
### 51.1 Viewing WAN Status

The **WAN Status** item allows you to view the WAN access status and Internet connection.

➤ **To view the status of the WAN connection:**

- Click the **WAN Status** item (**Status & Diagnostics** tab > **Data Status** menu > **WAN Status**); the following page appears:

**Figure 51-1: WAN Status**



The screenshot shows a window titled "WAN Access" with a green "Connected" status indicator in the top right corner. The window contains a table with the following information:

Technology:	Ethernet
Protocol:	Ethernet
Connection Speed:	1000.0 Mbps Full-Duplex
Connection Duration:	48 days, 23 hours
Internet Address:	195.189.192.72
Default Gateway:	195.189.192.65

The status of the WAN interface is depicted by the round icon located in the top-right corner:

- "Connected" (green): Valid connection to the WAN network.
- "Cable Disconnected" (red): A WAN connection is configured but there is no physical connection to the WAN (i.e., cable disconnected).
- "No Internet Connection" (red): No WAN connection has been configured.

## 51.2 Viewing Network Connection Statistics

The Network Connections page displays a table summarizing the monitored connection data. The device constantly monitors traffic within the local network and between the local network and the Internet. You can view statistical information about data received from and transmitted to the Internet (WAN) and to computers in the local network (LAN).

➤ **To view data on network connections:**

- Click the **Connection Statistics** item (**Status & Diagnostics** tab > **Data Status** menu > **Connection Statistics**); the following page appears:

**Figure 51-2: Connection Statistics Page**

Name	LAN Switch	LAN Switch VLAN 1	WAN Ethernet	LAN Switch VLAN 4001
Device Name	eth0	eth0.1	eth1	eth0.4001
Status	1 Ports Connected	Connected	Connected	Connected
Network	LAN	LAN	WAN	LAN
Underlying Device/s		LAN Switch		LAN Switch
Connection Type	Hardware Ethernet Switch	Ethernet	Ethernet	Ethernet
Download Rate	100 Mbps	100 Mbps	1000 Mbps	100 Mbps
Upload Rate	100 Mbps	100 Mbps	1000 Mbps	100 Mbps
MAC Address	00:90:8f:2e:59:58	00:90:8f:2e:59:58	00:90:8f:2e:59:59	00:90:8f:2e:59:58
IP Address		10.62.0.73	195.189.192.72	169.254.254.253
Subnet Mask		255.255.0.0	255.255.255.240	255.255.255.252
DNS Server			195.189.192.65 80.179.52.100 80.179.55.100	
IP Address Distribution	Disabled	Disabled	Disabled	Disabled
Received Packets	3891932	1513474	2592488	9821713
Sent Packets	6596920	11624	8445	6585109
Received Bytes	360047409	141871751	202006770	818875895
Sent Bytes	3644952014	534824	2600715	3644281744
Receive Errors	0	0	0	0
Receive Drops	0	0	0	0
Time Span	1175:24:38	1175:24:05	1175:24:38	1175:24:04

To update the display, click the **Refresh** button, or click the **Automatic Refresh On** button to constantly update the displayed parameters.

## 51.3 Viewing Logged Security Events

The **Security Log** item displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate through an administrative interface (Web or Telnet terminal), firewall configuration and system start-up.

➤ **To view logs of firewall-related events:**

1. Click the **Security Log** item (**Status & Diagnostics** tab > **Data Status** menu > **Security Log**); the following page appears:

**Figure 51-3: Firewall - Log Page**

Time	Event	Event-Type	Details
Jan 1 17:25:25 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 1 17:25:25 2003	Firewall Setup	Firewall internal	Starting firewall configuration
Jan 1 17:25:25 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 1 17:25:25 2003	Firewall Setup	Firewall internal	Starting firewall configuration
Jan 1 00:00:07 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded

The log table displays the following details:

- **Time:** time the event occurred.
- **Event:** there are five kinds of events:
  - ◆ **Inbound Traffic:** event is a result of an incoming packet.
  - ◆ **Outbound Traffic:** event is a result of outgoing packet.
  - ◆ **Firewall Setup:** configuration message
  - ◆ **WBM Login:** indicates that a user has logged in to the Web interface.
  - ◆ **CLI Login:** indicates that a user has logged in to CLI (via Telnet).
- **Event-Type:** textual description of the event:
  - ◆ **Blocked:** packet was blocked (message is colored red).
  - ◆ **Accepted:** packet was accepted (message is colored green).
- **Details:** additional details about the packet or the event such as protocol, IP addresses, ports, etc.

The page also provides you with the following buttons:

- **Clear Log:** clears currently displayed log messages from the table.
- **Refresh:** updates the log display with the latest log messages.
- **Settings:** allows you to select the types of activities for which you want to have a log message generated, as shown below:

**Figure 51-4: Log Settings Page**

Accepted Events		
<input type="checkbox"/>	Accepted Incoming Connections	
<input type="checkbox"/>	Accepted Outgoing Connections	

Blocked Events		
<input type="checkbox"/>	All Blocked Connection Attempts	
<input type="checkbox"/>	Winnuke	<input type="checkbox"/> Multicast/Broadcast
<input type="checkbox"/>	Defragmentation Error	<input type="checkbox"/> Spoofed Connection
<input type="checkbox"/>	Blocked Fragments	<input type="checkbox"/> Packet Illegal Options
<input type="checkbox"/>	Syn Flood	<input type="checkbox"/> UDP Flood
<input type="checkbox"/>	Echo Chargen	<input type="checkbox"/> ICMP Replay
		<input checked="" type="checkbox"/> ICMP Redirect
		<input type="checkbox"/> ICMP Multicast
		<input type="checkbox"/> ICMP Flood

Other Events	
<input type="checkbox"/>	Remote Administration Attempts
<input type="checkbox"/>	Connection States

Log Buffer	
<input type="checkbox"/>	Prevent Log Overrun

- Accepted Events group:
  - ◆ **Accepted Incoming Connections:** generates a log message for each successful attempt to establish an inbound connection to the home network.
  - ◆ **Accepted Outgoing Connections:** generates a log message for each successful attempt to establish an outgoing connection to the public network.
- Blocked Events group:
  - ◆ **All Blocked Connection Attempts:** generates a log message for each blocked attempt to establish an inbound connection to the home network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options listed below it.
  - ◆ Generate a log message for specific events that are blocked such as SynFlood. A log message is generated if either the corresponding check box is checked, or the 'All Blocked Connection Attempts' check box is selected.
- Other Events group:
  - ◆ **Remote Administration Attempts:** generates a log message for each remote administration connection attempt, whether successful or not.
  - ◆ **Connection States:** provide additional information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and Application Level Gateways (ALGs).
- Log Buffer group:
  - ◆ **Prevent Log Overrun:** stops logging firewall activities when the memory allocated for the log fills up.

## 51.4 Viewing QoS Queues Statistics

You can view an accurate, real-time information on the traffic moving through your defined device classes. For example, the amount of packets sent, dropped or delayed are just a few of the parameters that you can monitor per shaping class.

➤ **To view your class statistics:**

- Click the **QoS Class Statistics** item (**Status & Diagnostics** tab > **Data Status** menu > **QoS Queues Statistics**); the following page appears:

**Figure 51-5: QoS Queues Statistics Page**



**Note:** Class statistics are only available after defining at least one class; otherwise, the page does not display any information.

## 51.5 Viewing Logged Data Events

The **Data Log** item displays a list of recent events occurred on the device.

➤ **To view logged messages:**

- Click the **Data Log** item (**Status & Diagnostics** tab > **Data Status** menu > **Data Log**); the following page appears:

**Figure 51-6: System Log Page**

Time	Component	Severity	Details
Jan 1 17:25:25 2003	DHCP	Information	Activated Server for dev eth0
Jan 1 00:00:15 2003	IPSec	Information	pluto[57]: RATELIMIT: 1 messages of type IPSec IKE packet reported 11 second(s) ago
Jan 1 00:00:07 2003	Main Task	Information	eth1: link up, device will be up

By default, all log messages are displayed one after another, sorted by their order of posting by the device (latest on top). You can sort the messages according to the column titles 'Time', 'Component', or 'Severity', by clicking the column header. You can also filter the log messages by the component that generated them or by their severity, providing a more refined list. By default, the page displays log messages with 'debug' severity level and higher, for all components. You may change the severity level for this filter.

➤ **To add a new log display filter:**

1. In the 'Filters' group, click the **New Filter** link; the 'Filters' group displays a new Component entry.

**Figure 51-7: Adding a New Filter**



Component	Severity	Action
All	Information	
Other	Information	✖

[New Filter](#)

2. Using the drop-down lists, select the component and severity level by which to sort the log messages.
3. Click **Apply Filters** to display the messages in your specified criteria.

You can also delete filters using their respective action icons. Clicking **Reset Filters** deletes all the defined filters. Defined filters override the default filter that displays all messages.

You can use the buttons located at the top of the page to perform the following:

- **Close:** closes the 'Log page and returns to the device's Home page.
- **Clear Log:** clears all currently displayed log messages.
- **Refresh:** refreshes the page to display the latest log messages.



## 52 Reporting Information to External Party

This section describes features for reporting various information to an external party.

### 52.1 RTP Control Protocol Extended Reports (RTCP XR)

RTP Control Protocol Extended Reports (RTCP XR) is a VoIP management control that defines a set of metrics containing information for assessing VoIP call quality and for diagnosing problems. RTCP XR (RFC 3611) extends the RTCP reports defined in RFC 3550 by providing additional VoIP metrics. RTCP XR information publishing is implemented in the device according to <draft-johnston-sipping-rtcp-summary-07>. This draft defines how a SIP User Agent (UA) publishes the detailed information to a defined collector. RTCP XR measures VoIP call quality such as packet loss, delay, signal / noise / echo levels, estimated R-factor, and mean opinion score (MOS). RTCP XR measures these parameters using metrics as listed in the table below.



**Note:** RTCP XR is a customer ordered feature and thus, must be included in the Software License Key installed on the device.

RTCP XR messages containing key call-quality-related metrics are exchanged periodically (user-defined) between the device and the SIP UA. This allows an analyzer to monitor these metrics midstream, or a device to retrieve them using SNMP. The device can send RTCP XR reports to an Event State Compositor (ESC) server using PUBLISH messages. These reports can be sent at the end of each call and according to a user-defined interval between consecutive reports.

**RTCP XR Published VoIP Metrics**

Group	Metric Name
<b>General</b>	Start Timestamp
	Stop Timestamp
	Call-ID
	Local Address (IP, Port & SSRC)
	Remote Address (IP, Port & SSRC)
<b>Session Description</b>	Payload Type
	Payload Description
	Sample Rate
	Frame Duration
	Frame Octets
	Frames per Packets
	Packet Loss Concealment
	Silence Suppression State
<b>Jitter Buffer</b>	Jitter Buffer Adaptive
	Jitter Buffer Rate

Group	Metric Name
	Jitter Buffer Nominal
	Jitter Buffer Max
	Jitter Buffer Abs Max
<b>Packet Loss</b>	Network Packet Loss Rate
	Jitter Buffer Discard Rate
<b>Burst Gap Loss</b>	Burst Loss Density
	Burst Duration
	Gap Loss Density
	Gap Duration
	Minimum Gap Threshold
<b>Delay</b>	Round Trip Delay
	End System Delay
	One Way Delay
	Interarrival Jitter
	Min Absolute Jitter
	Signal
	Signal Level
	Noise Level
	Residual Echo Return Noise
<b>Quality Estimates</b>	Listening Quality R
	RLQ Est. Algorithm
	Conversational Quality R
	RCQ Est. Algorithm
	External R In
	Ext. R In Est. Algorithm
	External R Out
	Ext. R Out Est. Algorithm
	MOS-LQ
	MOS-LQ Est. Algorithm
	MOS-CQ
	MOS-CQ Est. Algorithm
	QoE Est. Algorithm

➤ **To configure RTCP XR:**

1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** > **RTP/RTCP Settings**). The RTCP XR parameters are listed under the 'RTCP XR Settings' group, as shown below:

**Figure 52-1: RTCP XR Parameters in RTP/RTCP Settings Page**

▼ RTCP XR Settings	
Burst Threshold	-1
Delay Threshold	-1
R-Value Delay Threshold	-1
⚡ Enable RTCP XR	CE_VQMON_DISABLE ▼
Minimum Gap Size	16
RTCP XR Report Mode	Disable ▼
RTCP XR Packet Interval	0
Disable RTCP XR Interval Randomization	Disable ▼
RTCP XR Collection Server	
RTCP XR Collection Server Transport Type	Not Configured ▼

2. Configure the RTCP XR parameters, as required:
  - 'Enable RTCP XR' (*VQMonEnable*) - enables voice quality monitoring and RTCP XR.
  - 'Minimum Gap Size' (*VQMonGMin*) - defines the voice quality monitoring - minimum gap size (number of frames).
  - 'Burst Threshold' (*VQMonBurstTHR*) - defines the voice quality monitoring - excessive burst alert threshold.
  - 'Delay Threshold' (*VQMonDelayTHR*) - defines the voice quality monitoring - excessive delay alert threshold.
  - 'R-Value Delay Threshold' (*VQMonEOCRValTHR*) - defines the voice quality monitoring - end of call low quality alert threshold.
  - 'RTCP XR Report Mode' (*RTCPXRReportMode*) - determines whether RTCP XR reports are sent to the ESC and defines the interval in which they are sent.
  - 'RTCP XR Packet Interval' (*RTCPInterval*) - defines the time interval between adjacent RTCP reports.
  - 'Disable RTCP XR Interval Randomization' (*DisableRTCPRandomize*) - determines whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter RTCPInterval.
  - 'RTCP XR Collection Server' (*RTCPXREscIP*) - defines the IP address of the Event State Compositor (ESC).
  - 'RTCP XR Collection Server Transport Type' (*RTCPXRESCTransportType*) - determines the transport layer for outgoing SIP dialogs initiated by the device to the RTCP XR Collection Server.
3. Click **Submit**.
4. Reset the device for the settings to take effect.

## 52.2 Generating Call Detail Records

The Call Detail Record (CDR) contains vital statistic information on calls made from the device. The device can be configured to generate and report CDRs for various stages of the call, including SIP messages and/or media. You can configure when CDRs for a call are generated, for example, only at the end of the call or only at the start and end of the call. Once generated, the device sends the CDRs to a user-defined Syslog server.

The CDR Syslog message complies with RFC 3161 and is identified by Facility 17 (local1) and Severity 6 (Informational).

For CDR in RADIUS format, see 'RADIUS Accounting CDR Attributes' on page 619.

### 52.2.1 Configuring CDR Reporting

The procedure below describes how to configure CDR reporting.

➤ **To configure CDR reporting:**

1. Enable the Syslog feature for sending log messages generated by the device to a collecting log message server. For more information, see 'Configuring Syslog' on page 629.
2. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**). The CDR parameters appear under the 'CDR and Debug' group, as shown below:

**Figure 52-2: CDR Parameters in Advanced Parameters Page**

CDR and Debug	
CDR Server IP Address	10.8.6.55
CDR Report Level	Start & End & Connect Call ▼
Media CDR Report Level	End Media ▼

3. Configure the parameters as required. For a description of the parameters, see 'Syslog, CDR and Debug Parameters' on page 680.
4. Click **Submit**.



**Note:** If the CDR server IP address is not configured, the CDRs are sent to the Syslog server, configured in 'Configuring Syslog' on page 629.

## 52.2.2 CDR Field Description

This section describes the CDR fields that are generated by the device.

### 52.2.2.1 CDR Fields for SBC Signaling

The CDR fields for SBC signaling are listed in the table below. The signaling CDRs are published for each SBC leg.

**CDR Fields for SBC Signaling**

CDR Field Name	Description
<b>SBCReportType</b>	Report Type: <ul style="list-style-type: none"><li>▪ <b>CALL_START</b></li><li>▪ <b>CALL_CONNECT</b></li><li>▪ <b>CALL_END</b></li><li>▪ <b>DIALOG_START</b></li><li>▪ <b>DIALOG_END</b></li></ul>
<b>EPTyp</b>	Endpoint type ( <b>SBC</b> )
<b>SIPMethod</b>	SIP message type
<b>SIPCallId</b>	Unique ID of call
<b>SessionId</b>	Unique Session ID
<b>Orig</b>	Call originator: <ul style="list-style-type: none"><li>▪ <b>LCL</b> - for local</li><li>▪ <b>RMT</b> - for remote</li></ul>
<b>SourceIp</b>	Source IP address
<b>SourcePort</b>	Source UDP port
<b>DestIp</b>	Destination IP address
<b>DestPort</b>	Destination UDP port
<b>TransportType</b>	Transport type: <ul style="list-style-type: none"><li>▪ <b>UDP</b></li><li>▪ <b>TCP</b></li><li>▪ <b>TLS</b></li></ul>
<b>SrcURI</b>	Source URI
<b>SrcURIBeforeMap</b>	Source URI before manipulation
<b>DstURI</b>	Destination URI
<b>DstURIBeforeMap</b>	Destination URI before manipulation
<b>Durat</b>	Call duration
<b>TrmSd</b>	Termination side (local or remote)
<b>TrmReason</b>	Termination reason

CDR Field Name	Description
<b>TrmReasonCategory</b>	Termination reason category: <ul style="list-style-type: none"> <li> Calls with duration 0 (i.e., not connected): <ul style="list-style-type: none"> <li>✓ <b>NO_ANSWER</b> - GWAPP_NORMAL_CALL_CLEAR, GWAPP_NO_USER_RESPONDING, GWAPP_NO_ANSWER_FROM_USER_ALERTED</li> <li>✓ <b>BUSY</b> - GWAPP_USER_BUSY</li> <li>✓ <b>NO_RESOURCES</b> - GWAPP_RESOURCE_UNAVAILABLE_UNSPECIFIED, RELEASE_BECAUSE_NO_CONFERENCE_RESOURCES_LEFT, RESOURCE_BECAUSE_NO_TRANSCODING_RESOURCES_LEFT, RELEASE_BECAUSE_GW_LOCKED</li> <li>✓ <b>NO_MATCH</b> - RELEASE_BECAUSE_UNMATCHED_CAPABILITIES</li> <li>✓ <b>FORWARDED</b> - RELEASE_BECAUSE_FORWARD</li> <li>✓ <b>GENERAL_FAILED</b> - any other reason</li> </ul> </li> <li> Calls with duration: <ul style="list-style-type: none"> <li>✓ <b>NORMAL_CALL_CLEAR</b> - GWAPP_NORMAL_CALL_CLEAR</li> <li>✓ <b>ABNORMALLY_TERMINATED</b> - Anything else</li> </ul> </li> <li><b>N/A</b> - Reasons not belonging to above categories</li> </ul>
<b>SetupTime</b>	Call setup time
<b>ConnectTime</b>	Call connect time
<b>ReleaseTime</b>	Call release time
<b>RedirectReason</b>	Redirect reason
<b>RedirectURINum</b>	Redirection URI
<b>RedirectURINumBeforeMap</b>	Redirect URI number before manipulation
<b>TxSigIPDiffServ</b>	Signaling IP DiffServ
<b>IPGroup</b>	IP Group description
<b>SrdId</b>	SRD name
<b>SIPInterfaceId</b>	SIP Interface ID
<b>ProxySetId</b>	Proxy Set ID
<b>IpProfileId</b>	IP Profile name
<b>MediaRealmId</b>	Media Realm name
<b>DirectMedia</b>	Direct media or traversing SBC: <ul style="list-style-type: none"> <li>yes</li> <li>no</li> </ul>
<b>SIPTrmReason</b>	SIP call termination reason (BYE, CANCEL, or SIP error codes, e.g., 404)

CDR Field Name	Description
<b>SipTermDesc</b>	<p>Description of SIP termination reason:</p> <ul style="list-style-type: none"> <li>SIP Reason header, if exists, for example: SIP ;cause=200 ;text="Call completed elsewhere".</li> <li>If no SIP Reason header exists, the description is taken from the reason text, if exists, of the SIP response code, for example: "417 Unknown Resource-Priority".</li> <li>If no reason text exists in the SIP response code, the description is 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.</li> </ul>

An example of an SBC signaling CDR sent by the device is shown below:

```
[S=1] |SBCReportType |EPTyp| SIPCallId| SessionId |Orig |SourceIp
|SourcePort |DestIp |DestPort |TransportType |SrcURI
|SrcURIBeforeMap |DstURI |DstURIBeforeMap |Durat |TrmSd |TrmReason
|TrmReasonCategory |SetupTime |ConnectTime |ReleaseTime
|RedirectReason |RedirectURINum |RedirectURINumBeforeMap
|TxSigIPDiffServ |IPGroup (description) |SrdId (name)
|SIPInterfaceId |ProxySetId |IpProfileId (name) |MediaRealmId
(name) |DirectMedia |SIPTrmReason
[S=3] |CALL_END |SBC |170369730753201211288@10.132.10.245 |0 |RMT
|10.132.10.245 |5060 |10.132.10.250 |5070 |UDP |103@audiocodes.com
|103@audiocodes.com |101@10.132.10.250 |101@10.132.10.250 |0 |RMT
|GWAPP_NORMAL_CALL_CLEAR |NO_ANSWER |06:13:54.950 UTC Thu Mar 02
2012 | |06:14:01.175 UTC Thu Mar 02 2012 |-1 | | |40 |2 ( ) |0
(5070SRD) |2 |3 |0 ( ) |0 (lanmedia) |no |CANCEL
```

### 52.2.2.2 CDR Fields for SBC Media

The CDR fields for SBC media are listed in the table below. The media CDRs are published for each active media stream, thereby allowing multiple media CDRs, where each media CDR has a unique call ID corresponding to the signaling CDR.

**CDR Fields for SBC Media**

CDR Field Name	Description
<b>MediaReportType</b>	Report type (media start, update, or end)
<b>SIPCallId</b>	Unique call ID
<b>Cid</b>	Channel CID
<b>MediaType</b>	Media type (audio, video, or text)
<b>Coder</b>	Coder name
<b>PacketInterval</b>	Coder packet interval
<b>LocalRtpIp</b>	Local RTP IP address
<b>LocalRtpPort</b>	Local RTP port
<b>RemoteRtpIp</b>	Remote RTP IP address
<b>RemoteRtpPort</b>	Remote RTP port
<b>InPackets</b>	Number of received packets

CDR Field Name	Description
<b>OutPackets</b>	Number of sent packets
<b>LocalPackLoss</b>	Local packet loss
<b>RemotePackLoss</b>	Remote packet loss
<b>RTPdelay</b>	RTP delay
<b>RTPjitter</b>	RTP jitter
<b>TxRTPssrc</b>	Tx RTP SSRC
<b>RxRTPssrc</b>	Local RTP SSRC
<b>LocalRFactor</b>	Local conversation quality
<b>RemoteRFactor</b>	Remote conversation quality
<b>LocalMosCQ</b>	Local MOS for conversation
<b>RemoteMosCQ</b>	Remote MOS for conversation
<b>TxRTPIPDiffServ</b>	Media IP DiffServ
<b>LatchedRtplp</b>	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.
<b>LatchedRtpPort</b>	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.

### 52.2.2.3 CDR Fields for Gateway/IP-to-IP Application

The CDR fields for the Gateway / IP-to-IP application are listed in the table below.

**CDR Fields for Gateway/IP-to-IP Application**

Field Name	Description
<b>GWReportType</b>	Report type: <ul style="list-style-type: none"> <li>CALL_START</li> <li>CALL_CONNECT</li> <li>CALL_END</li> </ul>
<b>Cid</b>	Port number
<b>SessionId</b>	SIP session identifier
<b>Trunk</b>	Physical trunk number <b>Note:</b> This field is applicable only to the Gateway application.
<b>BChan</b>	Selected B-channel <b>Note:</b> This field is applicable only to the Gateway application.
<b>ConId</b>	SIP conference ID <b>Note:</b> This field is applicable only to the Gateway application.
<b>TG</b>	Trunk Group ID <b>Note:</b> This field is applicable only to the Gateway application.



Field Name	Description
<b>EPTyp</b>	Endpoint type: <ul style="list-style-type: none"> <li>▪ FXO</li> <li>▪ FXS</li> <li>▪ EANDM</li> <li>▪ ISDN</li> <li>▪ CAS</li> <li>▪ DAA</li> <li>▪ IPMEDIA</li> <li>▪ NETANN</li> <li>▪ STREAMING</li> <li>▪ TRANSPARENT</li> <li>▪ MSCML</li> <li>▪ VXML</li> <li>▪ IP2IP</li> </ul>
<b>Orig</b>	Call originator: <ul style="list-style-type: none"> <li>▪ LCL (Tel side)</li> <li>▪ RMT (IP side)</li> </ul>
<b>SourceIp</b>	Source IP address
<b>DestIp</b>	Destination IP address
<b>TON</b>	Source phone number type <b>Note:</b> This field is applicable only to the Gateway application.
<b>NPI</b>	Source phone number plan <b>Note:</b> This field is applicable only to the Gateway application.
<b>SrcPhoneNum</b>	Source phone number
<b>SrcNumBeforeMap</b>	Source number before manipulation
<b>TON</b>	Destination phone number type <b>Note:</b> This field is applicable only to the Gateway application.
<b>NPI</b>	Destination phone number plan <b>Note:</b> This field is applicable only to the Gateway application.
<b>DstPhoneNum</b>	Destination phone number
<b>DstNumBeforeMap</b>	Destination number before manipulation
<b>Durat</b>	Call duration
<b>Coder</b>	Selected coder
<b>Intrv</b>	Packet interval
<b>RtpIp</b>	RTP IP address
<b>Port</b>	Remote RTP port
<b>TrmSd</b>	Initiator of call release (IP, Tel, or Unknown)
<b>TrmReason</b>	SIP call termination reason (see 'Release Reasons in CDR' on page 616)
<b>Fax</b>	Fax transaction during call
<b>InPackets</b>	Number of incoming packets

Field Name	Description
<b>OutPackets</b>	Number of outgoing packets
<b>PackLoss</b>	Local packet loss
<b>RemotePackLoss</b>	Number of outgoing lost packets
<b>SIPCallId</b>	Unique SIP call ID
<b>SetupTime</b>	Call setup time
<b>ConnectTime</b>	Call connect time
<b>ReleaseTime</b>	Call release time
<b>RTPdelay</b>	RTP delay
<b>RTPjitter</b>	RTP jitter
<b>RTPssrc</b>	Local RTP SSRC
<b>RemoteRTPssrc</b>	Remote RTP SSRC
<b>RedirectReason</b>	Redirect reason
<b>TON</b>	Redirection phone number type <b>Note:</b> This field is applicable only to the Gateway application.
<b>NPI</b>	Redirection phone number plan <b>Note:</b> This field is applicable only to the Gateway application.
<b>RedirectPhonNum</b>	Redirection phone number
<b>MeteringPulses</b>	Number of generated metering pulses <b>Note:</b> This field is applicable only to the Gateway application.
<b>SrcHost</b>	Source host name
<b>SrcHostBeforeMap</b>	Source host name before manipulation
<b>DstHost</b>	Destination host name
<b>DstHostBeforeMap</b>	Destination host name before manipulation
<b>IPG</b>	IP Group description
<b>LocalRtpIp</b>	Remote RTP IP address
<b>LocalRtpPort</b>	Local RTP port
<b>Amount</b>	0-999999 Data is stored per call and sent in the syslog as follows: <ul style="list-style-type: none"> <li>currency-type: amount multiplier for currency charge (euro or usd)</li> <li>recorded-units: for unit charge (1-999999)</li> </ul>
<b>Mult</b>	0,001-1000 (in steps of 10) (See explanation above.)

Field Name	Description
<b>TrmReasonCategory</b>	<p>Termination reason category:</p> <ul style="list-style-type: none"> <li>▪ Calls with duration 0 (i.e., not connected): <ul style="list-style-type: none"> <li>✓ <b>NO_ANSWER</b> - GWAPP_NORMAL_CALL_CLEAR, GWAPP_NO_USER_RESPONDING, GWAPP_NO_ANSWER_FROM_USER_ALERTED</li> <li>✓ <b>BUSY</b> - GWAPP_USER_BUSY</li> <li>✓ <b>NO_RESOURCES</b> - GWAPP_RESOURCE_UNAVAILABLE_UNSPECIFIED, RELEASE_BECAUSE_NO_CONFERERENCE_RESOURCES_LEFT, RESOURCE_BECAUSE_NO_TRANSCODING_RESOURCES_LEFT, RELEASE_BECAUSE_GW_LOCKED</li> <li>✓ <b>NO_MATCH</b> - RELEASE_BECAUSE_UNMATCHED_CAPABILITIES</li> <li>✓ <b>FORWARDED</b> - RELEASE_BECAUSE_FORWARD</li> <li>✓ <b>GENERAL_FAILED</b> - any other reason</li> </ul> </li> <li>▪ Calls with duration: <ul style="list-style-type: none"> <li>✓ <b>NORMAL_CALL_CLEAR</b> - GWAPP_NORMAL_CALL_CLEAR</li> <li>✓ <b>ABNORMALLY_TERMINATED</b> - Anything else</li> </ul> </li> <li>▪ <b>N/A</b> - Reasons not belonging to above categories</li> </ul>
<b>RedirectNumBeforeMap</b>	Redirect number before manipulation
<b>SrdId</b>	SRD ID name
<b>SIPInterfaceId</b>	SIP interface ID
<b>ProxySetId</b>	Proxy Set ID
<b>IpProfileId</b>	IP Profile ID name
<b>MediaRealmId</b>	Media Realm name
<b>SigTransportType</b>	SIP signaling transport type (UDP, TCP, or TLS)
<b>TxRTPIPDiffServ</b>	Media IP DiffServ
<b>TxSigIPDiffServ</b>	Signaling IP DiffServ
<b>LocalRFactor</b>	Local R-factor
<b>RemoteRFactor</b>	Remote R-factor
<b>LocalMosCQ</b>	Local MOS for conversation quality
<b>RemoteMosCQ</b>	Remote MOS for conversation quality
<b>SigSourcePort</b>	SIP source port
<b>SigDestPort</b>	SIP destination port
<b>MediaType</b>	Media type - audio, video, or text
<b>SIPTrmReason</b>	SIP call termination reason (BYE, CANCEL, or SIP error codes, e.g., 404)

Field Name	Description
<b>SipTermDesc</b>	Description of SIP termination reason: <ul style="list-style-type: none"> <li>SIP Reason header, if exists, for example: SIP ;cause=200 ;text="Call completed elsewhere".</li> <li>If no SIP Reason header exists, the description is taken from the reason text, if exists, of the SIP response code, for example: "417 Unknown Resource-Priority".</li> <li>If no reason text exists in the SIP response code, the description is 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.</li> </ul>
<b>PstnTermReason</b>	Q.850 protocol termination reason (0-127).
<b>LatchedRtplp</b>	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.
<b>LatchedRtpPort</b>	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.

#### 52.2.2.4 Release Reasons in CDR

The possible reasons for call termination for the Gateway / IP-to-IP application which is represented in the CDR field **TrmReason** are listed below:

- "REASON N/A"
- "RELEASE\_BECAUSE\_NORMAL\_CALL\_DROP"
- "RELEASE\_BECAUSE\_DESTINATION\_UNREACHABLE"
- "RELEASE\_BECAUSE\_DESTINATION\_BUSY"
- "RELEASE\_BECAUSE\_NOANSWER"
- "RELEASE\_BECAUSE\_UNKNOWN\_REASON"
- "RELEASE\_BECAUSE\_REMOTE\_CANCEL\_CALL"
- "RELEASE\_BECAUSE\_UNMATCHED\_CAPABILITIES"
- "RELEASE\_BECAUSE\_UNMATCHED\_CREDENTIALS"
- "RELEASE\_BECAUSE\_UNABLE\_TO\_HANDLE\_REMOTE\_REQUEST"
- "RELEASE\_BECAUSE\_NO\_CONFERECE\_RESOURCES\_LEFT"
- "RELEASE\_BECAUSE\_CONFERECE\_FULL"
- "RELEASE\_BECAUSE\_VOICE\_PROMPT\_PLAY\_ENDED"
- "RELEASE\_BECAUSE\_VOICE\_PROMPT\_NOT\_FOUND"
- "RELEASE\_BECAUSE\_TRUNK\_DISCONNECTED"
- "RELEASE\_BECAUSE\_RSRC\_PROBLEM"
- "RELEASE\_BECAUSE\_MANUAL\_DISC"
- "RELEASE\_BECAUSE\_SILENCE\_DISC"
- "RELEASE\_BECAUSE\_RTP\_CONN\_BROKEN"
- "RELEASE\_BECAUSE\_DISCONNECT\_CODE"
- "RELEASE\_BECAUSE\_GW\_LOCKED"
- "RELEASE\_BECAUSE\_NORTEL\_XFER\_SUCCESS"
- "RELEASE\_BECAUSE\_FAIL"
- "RELEASE\_BECAUSE\_FORWARD"

- "RELEASE\_BECAUSE\_ANONYMOUS\_SOURCE"
- "RELEASE\_BECAUSE\_IP\_PROFILE\_CALL\_LIMIT"
- "GWAPP\_UNASSIGNED\_NUMBER"
- "GWAPP\_NO\_ROUTE\_TO\_TRANSIT\_NET"
- "GWAPP\_NO\_ROUTE\_TO\_DESTINATION"
- "GWAPP\_CHANNEL\_UNACCEPTABLE"
- "GWAPP\_CALL\_AWARDED\_AND "
- "GWAPP\_PREEMPTION"
- "PREEMPTION\_CIRCUIT\_RESERVED\_FOR\_REUSE"
- "GWAPP\_NORMAL\_CALL\_CLEAR"
- "GWAPP\_USER\_BUSY"
- "GWAPP\_NO\_USER\_RESPONDING"
- "GWAPP\_NO\_ANSWER\_FROM\_USER\_ALERTED"
- "MFCR2\_ACCEPT\_CALL"
- "GWAPP\_CALL\_REJECTED"
- "GWAPP\_NUMBER\_CHANGED"
- "GWAPP\_NON\_SELECTED\_USER\_CLEARING"
- "GWAPP\_INVALID\_NUMBER\_FORMAT"
- "GWAPP\_FACILITY\_REJECT"
- "GWAPP\_RESPONSE\_TO\_STATUS\_ENQUIRY"
- "GWAPP\_NORMAL\_UNSPECIFIED"
- "GWAPP\_CIRCUIT\_CONGESTION"
- "GWAPP\_USER\_CONGESTION"
- "GWAPP\_NO\_CIRCUIT\_AVAILABLE"
- "GWAPP\_NETWORK\_OUT\_OF\_ORDER"
- "GWAPP\_NETWORK\_TEMPORARY\_FAILURE"
- "GWAPP\_NETWORK\_CONGESTION"
- "GWAPP\_ACCESS\_INFORMATION\_DISCARDED"
- "GWAPP\_REQUESTED\_CIRCUIT\_NOT\_AVAILABLE"
- "GWAPP\_RESOURCE\_UNAVAILABLE\_UNSPECIFIED"
- "GWAPP\_PERM\_FR\_MODE\_CONN\_OUT\_OF\_S"
- "GWAPP\_PERM\_FR\_MODE\_CONN\_OPERATIONAL"
- "GWAPP\_PRECEDENCE\_CALL\_BLOCKED"
  - "RELEASE\_BECAUSE\_PREEMPTION\_ANALOG\_CIRCUIT\_RESERVED\_FOR\_REUSE"
  - "RELEASE\_BECAUSE\_PRECEDENCE\_CALL\_BLOCKED"
- "GWAPP\_QUALITY\_OF\_SERVICE\_UNAVAILABLE"
- "GWAPP\_REQUESTED\_FAC\_NOT\_SUBSCRIBED"
- "GWAPP\_BC\_NOT\_AUTHORIZED"
- "GWAPP\_BC\_NOT\_PRESENTLY\_AVAILABLE"
- "GWAPP\_SERVICE\_NOT\_AVAILABLE"
- "GWAPP\_CUG\_OUT\_CALLS\_BARRED"
- "GWAPP\_CUG\_INC\_CALLS\_BARRED"
- "GWAPP\_ACCES\_INFO\_SUBS\_CLASS\_INCONS"

- "GWAPP\_BC\_NOT\_IMPLEMENTED"
- "GWAPP\_CHANNEL\_TYPE\_NOT\_IMPLEMENTED"
- "GWAPP\_REQUESTED\_FAC\_NOT\_IMPLEMENTED"
- "GWAPP\_ONLY\_RESTRICTED\_INFO\_BEARER"
- "GWAPP\_SERVICE\_NOT\_IMPLEMENTED\_UNSPECIFIED"
- "GWAPP\_INVALID\_CALL\_REF"
- "GWAPP\_IDENTIFIED\_CHANNEL\_NOT\_EXIST"
- "GWAPP\_SUSPENDED\_CALL\_BUT\_CALL\_ID\_NOT\_EXIST"
- "GWAPP\_CALL\_ID\_IN\_USE"
- "GWAPP\_NO\_CALL\_SUSPENDED"
- "GWAPP\_CALL\_HAVING\_CALL\_ID\_CLEARED"
- "GWAPP\_INCOMPATIBLE\_DESTINATION"
- "GWAPP\_INVALID\_TRANSIT\_NETWORK\_SELECTION"
- "GWAPP\_INVALID\_MESSAGE\_UNSPECIFIED"
- "GWAPP\_NOT\_CUG\_MEMBER"
- "GWAPP\_CUG\_NON\_EXISTENT"
- "GWAPP\_MANDATORY\_IE\_MISSING"
- "GWAPP\_MESSAGE\_TYPE\_NON\_EXISTENT"
- "GWAPP\_MESSAGE\_STATE\_INCONSISTENCY"
- "GWAPP\_NON\_EXISTENT\_IE"
- "GWAPP\_INVALID\_IE\_CONTENT"
- "GWAPP\_MESSAGE\_NOT\_COMPATIBLE"
- "GWAPP\_RECOVERY\_ON\_TIMER\_EXPIRY"
- "GWAPP\_PROTOCOL\_ERROR\_UNSPECIFIED"
- "GWAPP\_INTERWORKING\_UNSPECIFIED"
- "GWAPP\_UNKNOWN\_ERROR"
- "RELEASE\_BECAUSE\_HELD\_TIMEOUT"

## 52.3 Configuring RADIUS Accounting

The device can send accounting data of SIP calls as call detail records (CDR) to a RADIUS Accounting server. The device can send the accounting messages to the RADIUS server upon call release, call connection and release, or call setup and release. For a list of the CDR attributes, see the table following the procedure below.



### Notes:

- For RADIUS accounting settings to take effect, you must save the settings to flash memory with a device reset.
- For a description of the RADIUS accounting parameters, see 'RADIUS Parameters' on page 695.

### ➤ To configure RADIUS accounting:

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

Figure 52-3: RADIUS Accounting Parameters Page

⚡ Enable RADIUS Access Control	Enable
Accounting Server IP Address	0.0.0.0
Accounting Port	1646
RADIUS Accounting Type	At Call Release
AAA Indications	None

- Configure the parameters as required.
- Click **Submit**.

The table below describes the RADIUS Accounting CDR attributes included in the communication packets transmitted between the device and a RADIUS server.

Supported RADIUS Accounting CDR Attributes

Attribute Number	Attribute Name	Vendor Specific Attribute (VSA) No.	Purpose	Value Format	Example	AAA
<b>Request Attributes</b>						
1	user-name	-	Account number or calling party number or blank	String up to 15 digits long	5421385747	Start Acc Stop Acc
4	nas-ip-address	-	IP address of the requesting device	Numeric	192.168.14.43	Start Acc Stop Acc
6	service-type	-	Type of service requested	Numeric	1: login	Start Acc Stop Acc
26	h323-incoming-conf-id	1	SIP call identifier	Up to 32 octets	-	Start Acc Stop Acc

Attribute Number	Attribute Name	Vendor Specific Attribute (VSA) No.	Purpose	Value Format	Example	AAA
26	h323-remote-address	23	IP address of the remote gateway	Numeric	-	Stop Acc
26	h323-conf-id	24	H.323/SIP call identifier	Up to 32 octets	-	Start Acc Stop Acc
26	h323-setup-time	25	Setup time in NTP format 1	String	-	Start Acc Stop Acc
26	h323-call-origin	26	The call's originator: Answering (IP) or Originator (PSTN)	String	Answer, Originate etc	Start Acc Stop Acc
26	h323-call-type	27	Protocol type or family used on this leg of the call	String	VoIP	Start Acc Stop Acc
26	h323-connect-time	28	Connect time in NTP format	String	-	Stop Acc
26	h323-disconnect-time	29	Disconnect time in NTP format	String	-	Stop Acc
26	H323-Disconnect-Cause	30	Q.931 disconnect cause code	Numeric	-	Stop Acc
26	h323-gw-id	33	Name of the gateway	String	SIPIDString	Start Acc Stop Acc
26	sip-call-id	34	SIP Call ID	String	abcde@ac.com	Start Acc Stop Acc
26	call-terminator	35	The call's terminator: PSTN-terminated call (Yes); IP-terminated call (No).	String	Yes, No	Stop Acc
30	called-station-id	-	Destination phone number (Gateway / IP-to-IP application) or Destination URI (SBC application)	String	8004567145	Start Acc
31	calling-station-id	-	Calling Party Number (ANI) (Gateway / IP-to-IP application) or Source URI (SBC application)	String	5135672127	Start Acc Stop Acc
40	acct-status-type	-	Account Request Type (start or stop) <b>Note:</b> 'start' isn't supported on the Calling Card application.	Numeric	1: start, 2: stop	Start Acc Stop Acc



Attribute Number	Attribute Name	Vendor Specific Attribute (VSA) No.	Purpose	Value Format	Example	AAA
41	acct-delay-time	-	No. of seconds tried in sending a particular record	Numeric	5	Start Acc Stop Acc
42	acct-input-octets	-	Number of octets received for that call duration (Gateway / IP-to-IP application)	Numeric	-	Stop Acc
43	acct-output-octets	-	Number of octets sent for that call duration (Gateway / IP-to-IP application)	Numeric	-	Stop Acc
44	acct-session-id	-	A unique accounting identifier - match start & stop	String	34832	Start Acc Stop Acc
46	acct-session-time	-	For how many seconds the user received the service	Numeric	-	Stop Acc
47	acct-input-packets	-	Number of packets received during the call	Numeric	-	Stop Acc
48	acct-output-packets	-	Number of packets sent during the call	Numeric	-	Stop Acc
61	nas-port-type	-	Physical port type of device on which the call is active	String	0: Asynchronous	Start Acc Stop Acc
<b>Response Attributes</b>						
26	h323-return-code	103	The reason for failing authentication (0 = ok, other number failed)	Numeric	0 Request accepted	Stop Acc
44	acct-session-id	-	A unique accounting identifier – match start & stop	String	-	Stop Acc

Below is an example of RADIUS Accounting, where the non-standard parameters are preceded with brackets:

```
Accounting-Request (361)
user-name = 111
acct-session-id = 1
nas-ip-address = 212.179.22.213
nas-port-type = 0
acct-status-type = 2
acct-input-octets = 4841
acct-output-octets = 8800
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
```

## 52.4 Querying Device Channel Resources using SIP OPTIONS

The device reports its maximum and available channel resources in SIP 200 OK responses upon receipt of SIP OPTIONS messages. The device sends this information in the SIP X-Resources header with the following parameters:

- **telchs:** Specifies the total telephone channels and the number of free (available) telephone channels.
- **mediachs:** Not applicable.

Below is an example of the X-Resources:

```
X-Resources: telchs= 12/4;mediachs=0/0
```

In the example above, "telchs" specifies the number of available channels and the number of occupied channels (4 channels are occupied and 12 channels are available).



**Note:** This feature is applicable only to the Gateway / IP-to-IP application.

# Part XIII

## Diagnostics



## 53 Syslog and Debug Recordings

Syslog is an event notification protocol that enables a device to send event notification messages across IP networks to event message collectors, also known as Syslog servers. The device contains an embedded Syslog client, which sends error reports / events that it generates to a remote Syslog server using the IP / UDP protocol. This information is a collection of error, warning, and system messages that records every internal operation of the device.

For receiving Syslog messages generated by the device, you can use any of the following Syslog servers:

- **Device's embedded Syslog server:** The device provides an embedded Syslog server, which is accessed through the Web interface. This provides limited Syslog server functionality.
- **Wireshark:** Third-party network protocol analyzer (<http://www.wireshark.org>).
- **Third-party, Syslog server:** Any third-party Syslog server program that enables filtering of messages according to parameters such as priority, IP sender address, time, and date.

### 53.1 Syslog Message Format

The Syslog message is sent from the device to a Syslog server as an ASCII (American Standard Code for Information Interchange) message. Syslog uses UDP as its underlying transport layer mechanism. By default, UDP port 514 is assigned to Syslog, but this can be changed (see 'Configuring Syslog' on page 629).

Below is an example of a Syslog message:

```
13:10:57.811 : 10.13.4.12 : NOTICE : [S=235][SID:1034099026] (
lgr_flow)(63          ) UdpTransportObject#0- Adding socket event
for address 10.33.2.42:5060 [Time: 04-19-2012@18:29:39]
```

**Syslog Message Format Description**

Message Item	Description
<b>Message Types</b>	<p>Syslog generates the following types of messages:</p> <ul style="list-style-type: none"> <li>■ <b>ERROR:</b> Indicates that a problem has been identified that requires immediate handling.</li> <li>■ <b>WARNING:</b> Indicates an error that might occur if measures are not taken to prevent it.</li> <li>■ <b>NOTICE:</b> Indicates that an unusual event has occurred.</li> <li>■ <b>INFO:</b> Indicates an operational message.</li> <li>■ <b>DEBUG:</b> Messages used for debugging.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>■ The INFO and DEBUG messages are required only for advanced debugging. Therefore, by default, they are not sent by the device.</li> <li>■ When viewing Syslog messages in the Web interface, these message types are color coded.</li> </ul>
<b>Message Sequence Number [S=&lt;number&gt;]</b>	<p>Syslog messages are sequentially numbered in the format [S=&lt;number&gt;], for example, "[S=643]".</p> <p>A skip in the number sequence of messages indicates a loss of message packets. For example, in the below Syslog message generation, messages 238 through 300 were not received. In other words, three Syslog messages were lost</p>

Message Item	Description
	<p>(the sequential numbers are indicated below in bold font):</p> <pre> 18:38:14. 52 : 10.33.45.72 : NOTICE: [S=<b>235</b>][SID:1034099026] (lgr_psbrdex)(619) recv &lt;-- DIGIT(0) Ch:0 OnTime:0 InterTime:100 Direction:0 System:1 [File: Line:-1] 18:38:14. 83 : 10.33.45.72 : NOTICE: [S=<b>236</b>][SID:1034099026] (lgr_flow)(620) #0:DIGIT_EV [File: Line:-1] 18:38:14. 83 : 10.33.45.72 : NOTICE: [S=<b>237</b>][SID:1034099026] (lgr_flow)(621)   #0:DIGIT_EV [File: Line:-1] 18:38:14.958 : 10.33.45.72 : NOTICE: [S=<b>301</b>][SID:1034099026] (lgr_flow)(625)   #0:DIGIT_EV [File: Line:-1] </pre>
<b>Log Number (lgr)(number)</b>	Ignore this number; it has been replaced by the Message Sequence Number (described previously).
<b>Session ID</b>	<p>Automatically assigned (random), unique session identifier (session-id / SID) number per call in the CDR of sent Syslog messages and debug recording packets. This enables you to filter the information (such as SIP, Syslog, and media) according to the SID.</p> <ul style="list-style-type: none"> <li>Gateway/IP-to-IP application: A call session is considered either as a Tel-to-IP leg or an IP-to-Tel leg, where each leg is assigned a unique SID.</li> <li>SBC application: A session is considered as both the outgoing and incoming legs, where both legs share the same SID.</li> </ul> <p>The benefit of this unique numbering is that it enables you to filter the information (such as SIP, Syslog, and media) according to a specific SID.</p> <p><b>Note:</b> Forked legs and alternative legs share the same SID.</p>
<b>Message Body</b>	Describes the message.
<b>Timestamp</b>	When the Network Time Protocol (NTP) is enabled, a timestamp string [ <b>hour</b> :minutes:seconds] is added to all Syslog messages.

### 53.1.1 Event Representation in Syslog Messages

The Syslog message events that the device sends are represented by unique abbreviations. An example of an abbreviated event in a Syslog message indicating packet loss (PL) is shown below:

```

Apr  4 12:00:12 172.30.1.14 PL:5 [Code:3a002] [CID:3294] [Time:
20:17:00]

```

The table below lists these unique event abbreviations:

### 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
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

Error Abbreviation	Error Name Description
AC	Invalid Channel ID
AL	Invalid Header Length
AO	Invalid Codec Type
AP	Unknown Aggregation Payload Type
AR	Invalid Routing Flag Received

### 53.1.2 Unique Device Identification in Syslog Messages

The Syslog messages include a unique string to identify the device.

Syslog messages relating to VoIP functionality are marked with "host"; those relating to Data Routing are marked with "DATA".

```
12/12 12:46:40.921 : 10.8.5.70 : NOTICE : host: 10.8.5.78 (sip_stack)(24) Resource SIPMessage deleted - #267
```

```
11/24 08:14:09.311 : 10.3.2.100 : WARNING : DATA: Failed to set device eth0 netmask: Cannot assign requested address
```

### 53.1.3 Identifying AudioCodes Syslog Messages using Facility Levels

The device's Syslog messages can easily be identified and distinguished from Syslog messages from other equipment, by setting its Facility level. The Facility levels of the device's Syslog messages are numerically coded with decimal values. Facility level may use any of the "local use" facilities (0 through 7), according to RFC 3164. Implementing Facility levels is useful, for example, if you collect the device's as well as other equipments' Syslog messages on the same server. Therefore, in addition to filtering Syslog messages according to IP address, the messages can be filtered according to Facility level.

The Facility level is configured using the SyslogFacility ini file parameter, which provides the following options:

#### 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)
```



### 53.1.4 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:

**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:

## 53.2 Configuring Syslog Settings

The procedure below describes how to configure Syslog. This includes defining the Syslog server address as well as selecting the activities on the device (for example, a parameter value change) that you want reported to the server.



**Notes:**

- For configuring CDR reporting, see 'Configuring CDR Reporting' on page [608](#).
- For viewing Syslog messages in the Web interface, see 'Viewing Syslog Messages' on page [634](#).
- For a detailed description on the Syslog parameters, see 'Syslog, CDR and Debug Parameters' on page [680](#).
- To configure the network interface (WAN or VoIP LAN OAMP) from where the device sends Syslog messages to a Syslog server, use the OampDefaultNetworkSource parameter.

➤ **To configure Syslog :**

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

**Figure 53-1: Syslog Settings Page**

▼ Syslog Settings		
Enable Syslog	Enable	▼
Syslog Server IP Address	10.8.2.4	
Syslog Server Port	514	
Debug Level	5	▼
▼ Activity Types to Report via 'Activity Log' Messages		
Parameters Value Change	<input type="checkbox"/>	
Auxiliary Files Loading	<input type="checkbox"/>	
Device Reset	<input type="checkbox"/>	
Flash Memory Burning	<input type="checkbox"/>	
Device Software Update	<input type="checkbox"/>	
Access to Restricted Domains	<input type="checkbox"/>	
Non-Authorized Access	<input type="checkbox"/>	
Sensitive Parameters Value Change	<input type="checkbox"/>	
Login and Logout	<input type="checkbox"/>	

2. Enable the Syslog feature by setting the 'Enable Syslog' to **Enable**.
3. Define the Syslog server using the 'Syslog Server IP Address' and 'Syslog Server Port' parameters.
4. Configure the debug level using the 'Debug Level' parameter.
5. Under the 'Activity Types to Report ...' group, select the activities to report.
6. Click **Submit** to apply your changes.

## 53.3 Configuring Debug Recording

The device enables you to activate debug recording and send debug recording packets to a defined capturing server. When the debug recording is activated, the device duplicates all messages that are sent and/or received by it and then sends them to an external IP address. The debug recording can be done for different types of traffic for example, RTP/RTCP, T.38, ISDN, CAS, 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.



**Notes:**

- Debug recording is collected only on the device's OAMP interface.
- You can also save debug recordings to an external USB hard drive connected to the device's USB port. For more information, see USB Storage Capabilities on page 573.

➤ **To configure and activate debug recording:**

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

**Figure 53-2: Logging Settings Page**

Debug Recording	
Debug Recording Destination IP	10.13.4.22
Debug Recording Destination Port	925
Debug Recording Status	Start

2. Configure the debug capturing server using the 'Debug Recording Destination IP' and 'Debug Recording Destination Port' parameters.
3. From the 'Debug Recording Status' drop-down list, select **Start** to start the debug recording or **Stop** to end the recording.
4. Click **Submit** to apply your changes.

## 53.4 Filtering Syslog Messages and Debug Recordings

The device can filter Syslog messages and debug recording (DR) packets, sent by the device to a Syslog server and packet capturing application (such as Wireshark) respectively. This can be useful to reduce CPU consumption and minimize negative impact on VoIP performance.

You can configure up to 30 filtering rules, each based on a selected filtering criteria (e.g., an IP Group). Each filtering criteria can be configured with a range. For example, you can filter Syslog messages for IP Groups 1 through 4. For each filter criteria, you can enable or disable Syslog messages and debug recording.

Debug recording can also be filtered using various filtering criteria such as SIP signaling or signaling and media.

➤ **To configure logging filtering rules:**

1. Open the Logging Filters Table page (**Configuration** tab > **System** menu > **Logging** > **Logging Filters Table**).
2. Click the **Add** button; the Add Record dialog box appears:

**Figure 53-3: Logging Filters Table - Add Record Dialog Box**

Add Record	
Index	1
Type	Any Filter
Value	
Syslog	Enable
Capture Type	Signaling + Media
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Configure the logging filter, as required. See the table below for a description of the parameters.
4. Click **Submit** to save your changes.


**Notes:**

- To configure the Syslog debug level, use the 'Debug Level' parameter (see 'Configuring Syslog' on page 629).
- The Logging Filters table can also be configured using the table ini file parameter, LoggingFilters or the CLI command configure system > logging > logging-filters.

**Logging Filters Table Parameters Description**

Parameter	Description
Filter Type CLI: filter-type <b>[LoggingFilters_Type]</b>	<p>Defines the filter criteria.</p> <ul style="list-style-type: none"> <li>▪ <b>[1]</b> Any (default)</li> <li>▪ <b>[2]</b> Trunk ID = Filters according to a specified Trunk ID (applicable only to the Gateway application).</li> <li>▪ <b>[3]</b> Trunk Group ID = Filters according to a specified Trunk Group ID (Applicable only to the Gateway/IP-to-IP application).</li> <li>▪ <b>[4]</b> Trunk &amp; B-channel = Filters according to a specified Trunk and B-channel (applicable only to the Gateway/IP-to-IP application).</li> <li>▪ <b>[5]</b> FXS or FXO = Filters according to a specified FXS or FXO port.</li> <li>▪ <b>[6]</b> Tel-to-IP = Filters according to a specified Tel-to-IP routing rule listed in the Outbound IP Routing table (applicable only to the Gateway/IP-to-IP application).</li> <li>▪ <b>[7]</b> IP-to-Tel = Filters according to a specified IP-to-Tel routing rule listed in the Inbound IP Routing table (applicable only to the Gateway/IP-to-IP application).</li> <li>▪ <b>[8]</b> IP Group = Filters according to a specified IP Group ID listed in the IP Group table.</li> <li>▪ <b>[9]</b> SRD = Filters according to a specified SRD ID listed in the SRD table.</li> <li>▪ <b>[10]</b> Classification = Filters according to a specified Classification rule listed in the Classification table (applicable only to the SBC and application).</li> <li>▪ <b>[11]</b> IP-to-IP Routing = Filters according to a specified SBC IP-to-IP routing rule listed in the IP-to-IP Routing table (applicable only to the SBC application).</li> <li>▪ <b>[12]</b> User = Filters according to a specified user defined by username or user@host.</li> <li>▪ <b>[13]</b> IP Trace = Filters according to a specified IP network trace wireshark-like expression. For a detailed description on configuring IP traces, see 'Filtering IP Network Traces' on page 633.</li> </ul>

Parameter	Description
Value CLI: value [LoggingFilters_Value]	<p>Defines the value of the selected filtering type in the 'Filter Type' parameter. The value can be the following:</p> <ul style="list-style-type: none"> <li>▪ A single value</li> <li>▪ A range, using a hyphen "-" between the two values, e.g., "1-3"</li> <li>▪ Multiple, non-contiguous values, using commas "," between each value, e.g., "1,3,9"</li> <li>▪ Trunks and FXO/FXS pertaining to a module, using the syntax module number/port or port, for example: <ul style="list-style-type: none"> <li>▪ "1/2", means module 1, port 2</li> <li>▪ "1/[2-4]", means module 1, ports 2 through 4</li> </ul> </li> <li>▪ Any to indicate all</li> <li>▪ For IP trace expressions, see e 'Filtering IP Network Traces' on page 633</li> </ul>
Syslog CLI: syslog [LoggingFilters_Syslog]	<p>Enables Syslog messages for the defined logging filter:</p> <ul style="list-style-type: none"> <li>▪ [0] Disable (default)</li> <li>▪ [1] Enable</li> </ul>
Capture Type CLI: capture-type [LoggingFilters_CaptureType]	<p>Enables debug recordings for the defined logging filter and defines what to record:</p> <ul style="list-style-type: none"> <li>▪ [0] None (default)</li> <li>▪ [1] Signaling = Information related to signaling such as SIP signaling messages, Syslog, and CDR.</li> <li>▪ [2] Signaling &amp; Media = Signaling and media (RTP/RTCP/T.38).</li> <li>▪ [3] Signaling &amp; Media &amp; PCM = Signaling, media, and PCM (voice signals from and to TDM).</li> <li>▪ [4] PSTN trace = ISDN and CAS traces - applicable only for Trunk-related filters.</li> </ul>

### 53.4.1 Filtering IP Network Traces

You can filter Syslog and debug recording messages for IP network traces, by setting the 'Filter Type' parameter to **IP Trace** in the Logging Filters table. IP traces are used to record any IP stream, according to destination and/or source IP address, or port and Layer-4 protocol (UDP, TCP or any other IP type as defined by <http://www.iana.com>).

When the **IP Trace** option is selected, only the 'Value' parameter is applicable; the 'Syslog' and 'Capture Type' parameters are not relevant. The 'Value' parameter configures the Wireshark-like filtering expressions for your IP trace. The following Wireshark-like expressions are supported:

#### Supported Wireshark-like Expressions for 'Value' Parameter

Expression	Description
ip.src, ip.dst	Source and destination IP address
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

Expression	Description
udp.port, tcp.port	Transport layer
udp.srcport, tcp.srcport	Transport layer for source port
udp.dstport, tcp.dstport	Transport layer for destination port
and, &&, ==, <, >	Between expressions

Below are examples of configured expressions for the 'Value' parameter:

- udp && ip.addr==10.8.6.55
- ip.src==10.8.6.55 && udp.port>=5000 and udp.port<6000
- ip.dst==10.8.0.1/16
- ip.addr==10.8.6.40

For conditions requiring the "or" / "|" expression, add multiple table rows. For example, the Wireshark condition "(ip.src == 1.1.1.1 or ip.src == 2.2.2.2) and ip.dst == 3.3.3.3" can be configured using the following two table row entries:

1. ip.src == 1.1.1.1 and ip.dst == 3.3.3.3
2. ip.src == 2.2.2.2 and ip.dst == 3.3.3.3



**Note:** If the 'Value' field is left empty, the device will record all IP traffic types.

## 53.5 Viewing Syslog Messages

You can use the following tools to view the Syslog messages sent by the device:

- Web interface's Message Log page (see below).
- CLI -The device sends the error messages (e.g. Syslog messages) to the CLI console as well as to the original configured destination. Use the following commands:

```
debug log           ; Starts the debug
no debug log        ; Stops the debug
no debug log all     ; Stops all debug process
```

- Any third-party Syslog server (e.g., Wireshark).

The procedure below describes how to view Syslog messages in the Web interface.



### Notes:

- It's not recommended to keep a Message Log session open for a prolonged period. This may cause the device to overload. For prolonged (and detailed) debugging, use an external Syslog server.
- You can select the Syslog messages in this page, and copy and paste them into a text editor such as Notepad. This text file (.txt) can then be sent to AudioCodes Technical Support for diagnosis and troubleshooting.

➤ **To activate the Web interface's Message Log:**

1. Enable Syslog (see 'Configuring Syslog' on page 629).
2. Open the Message Log page (**Status & Diagnostics** tab > **System Status** menu > **Message Log**); the Message Log page is displayed and the log is activated.

**Figure 53-4: Message Log Page**

Log is Activated

```

11d:14h:43m:9s ( lgr_psbrdex) (2662 ) recv <-- ON_HOOK Ch:1
11d:14h:43m:9s ( lgr_flow) (2663 ) #1:ON_HOOK_EV
11d:14h:43m:9s ( lgr_flow) (2664 ) | #1:ON_HOOK_EV
11d:14h:43m:9s ( lgr_psbrdif) (2665 ) #1:cpDigitMapHndlr_Stop - Stopped (0)
11d:14h:43m:9s ( lgr_psbrdif) (2666 ) #1:CloseChannel: ChannelNum=1
11d:14h:43m:9s ( lgr_psbrdif) (2667 ) Open channel: IsVoiceOn: 1, IsT38On: 1, IsVbdOn: 0, Is
11d:14h:43m:9s ( lgr_psbrdif) (2668 ) #1:OpenChannel:on Trunk -1 BChannel:1 CID=1 with Voice
11d:14h:43m:9s ( lgr_psbrdif) (2669 ) #1:OpenChannel VoiceVolume= 0, DTMFVolume = -11, Input
11d:14h:43m:9s ( lgr_psbrdif) (2670 ) OpenChannel, CoderType = 15, Interval = 4, M = 1
11d:14h:43m:9s ( lgr_psbrdif) (2671 ) #1:FAXTransportType = 1
11d:14h:43m:9s ( lgr_psbrdif) (2672 ) #1:ConfigFaxModemChannelParams NSEMode=0, CNGDetMode=0
11d:14h:43m:9s ( lgr_psbrdif) (2673 ) Detectors: Amd:0, Ans:0 En:0 IBScmd:Oxal
11d:14h:43m:9s ( lgr_psbrdif) (2674 ) #1:PSOSBoardInterface::StopPlayTone- Called
11d:14h:43m:9s ( lgr_psbrdex) (2675 ) recv <-- OFF_HOOK Ch:1
11d:14h:43m:9s ( lgr_flow) (2676 ) #1:OFF_HOOK_EV
11d:14h:43m:9s ( lgr_flow) (2677 ) | #1:OFF_HOOK_EV
11d:14h:43m:9s ( lgr_psbrdif) (2678 ) UpdateChannelParams, Channel 1
11d:14h:43m:9s ( lgr_psbrdif) (2679 ) #1:ConfigFaxModemChannelParams NSEMode=0, CNGDetMode=0
11d:14h:43m:9s ( lgr_psbrdif) (2680 ) ActivateDigitMap for channel : 1, MaxDialStringLength

```

The displayed logged messages are color-coded as follows:

- Yellow - fatal error message
- Blue - recoverable error message (i.e., non-fatal error)
- Black - notice message

➤ **To stop and clear the Message Log:**

- Close the Message Log page by accessing any another page in the Web interface.

## 53.6 Collecting Debug Recording Messages

To collect debug recording packets, the open source program Wireshark is used. AudioCodes proprietary plug-in files for Wireshark, which are shipped in your software kit, are also required.



### Notes:

- The default debug recording port is 925. You can change the port in Wireshark (**Edit menu > Preferences > Protocols > AC DR**).
- The plug-ins are per major software release and are applicable to Wireshark Ver. 1.62.
- The plug-ins are backward compatible.
- From Wireshark Ver. 99.08, the tpncp.dat file must be located in the folder, ...WireShark\tpncp.

### ➤ To install Wireshark and the plug-ins for debug recording:

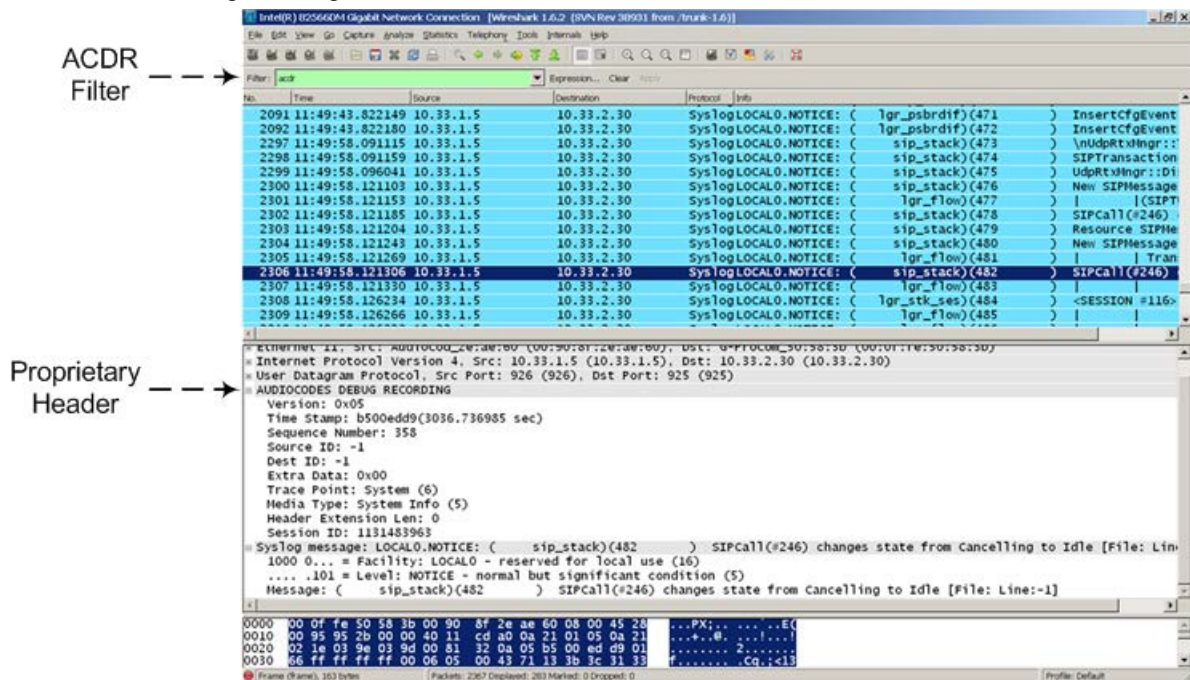
1. Install Wireshark on your computer. The Wireshark program can be downloaded from <http://www.wireshark.org>.
2. Copy the supplied AudioCodes plug-in files to the directory in which you installed Wireshark, as follows:

Copy this file	To this folder
...\dtds\cdr.dtd	Wireshark\dtds\
...\plugins\1.6.2\*.dll	Wireshark\plugins\1.6.2
...\tpncp\tpncp.dat	Wireshark\tpncp

3. Start Wireshark.
4. In the Filter field, type "acdr" (see the figure below) to view the debug recording messages. Note that the source IP address of the messages is always the OAMP IP address of the device.



The device adds the header "AUDIOCODES DEBUG RECORDING" to each debug recording message, as shown below:



For ISDN trace messages, the additional header, "NetBricks Trace" is added below the "AUDIOCODES DEBUG RECORDING" header, as shown in the example below:

```
AUDIOCODES DEBUG RECORDING
NetBricks Trace
System time: 3559
  Direction: Message received from internal server queue (73)
From (Entity origination ID): DL_D (DL LAPD Q.921) (100)
To (Entity destination ID): PH_D (D channel physical) (68)
Primitive code: 67
NAI (Network Access ID): 0 -> number of trunk
SAPI: 1
Connection ID: 0
Congestion flag: 0
Allocated message: 2
Allocated buffer: 3
Allocated timer cell: 141
IT Message stack counter: 120
IT Buffer stack counter: 120
Message congestion counter: 0
Buffer congestion counter: 0
IT Stack message congestion counter: 0
IT Stack buffer congestion counter: 0
Pointer to message: 689
Pointer to buffer: 0
Data size: 33
Link Access Procedure, Channel D (LAPD)
Q.931
  Protocol discriminator: Q.931
  Call reference value length: 2
  Call reference flag: Message sent from originating side
  Call reference value: 0300 - > can be used as a filter to
identify entire ISDN call
  Message type: SETUP (0x05)
  Bearer capability
```

```
Channel identification
Calling party number: '201'
Called party number: '102'
Sending complete
```

For CAS trace messages, the additional header "CAS Trace" is added below the "AUDIOCODES DEBUG RECORDING" header, as shown in the example below:

```
AUDIOCODES DEBUG RECORDING
CAS Trace
Timer: 1145504439
From: DSP (0)
Current State: 7
Event: EV_DIAL_ENDED (15)
Next State: -1
Function Use: Unknown (-1)
    Parameter 1: -1
    Parameter 2: -1
    Parameter 3: -1
Trunk Number: 3
BChannel Number: 23
Call Handle: 0
```

## 53.7 Capturing VoIP and Data-Router Network Traffic

You can capture VoIP and data-router network traffic by sending traces to the CLI or to a file that is later sent to a TFTP server. The traffic can be captured using the following CLI commands to start the debug capture process:

```
debug capture voip
debug capture data
```

## 54 Self-Testing

The device features the following self-testing modes to identify faulty hardware components:

- **Detailed Test (Configurable):** This test verifies the correct functioning of the different hardware components on the device. This test is done when the device is taken out of service (i.e., not in regular service for processing calls). The test is performed on startup when initialization of the device completes.

To enable this test, set the ini file parameter, EnableDiagnostics to 1 or 2, and then reset the device. Upon completion of the test and if the test fails, the device sends information on the test results of each hardware component to the Syslog server.

The following hardware components are tested:

- RAM - when EnableDiagnostics = 1 or 2
- Flash memory - when EnableDiagnostics = 1 or 2
- DSPs - when EnableDiagnostics = 1 or 2
- Physical Ethernet ports - when EnableDiagnostics = 1 or 2
- Analog interfaces - when EnableDiagnostics = 1 or 2



**Notes:**

- To return the device to regular operation and service, disable the test by setting the ini file parameter, EnableDiagnostics to 0, and then reset the device.
- While the test is enabled, ignore errors sent to the Syslog server.

- **Startup Test (automatic):** This hardware test has minor impact in real-time. While this test is executed, the regular operation of the device is disabled. If an error is detected, an error message is sent to the Syslog.

## Reader's Notes

## 55 Analog Line Testing

The device can test the telephone lines connected to its FXS and FXO ports, using the SNMP `acAnalogFxsLineTestTable` table and `acAnalogFxoLineTestTable` table respectively. These tests provide various line measurements. In addition to these tests (detailed below), a keep-alive test is also done every 100 msec on each of the analog ports to detect communication problems with the analog equipment and overheating of the FXS ports.

■ FXS line tests:

- Hardware revision number
- Temperature (above or below limit, only if a thermometer is installed)
- Hook state
- Coefficients checksum
- Message waiting indication status
- Ring state
- Reversal polarity state

■ FXO line tests:

- Line Current (mA)
- Line Voltage (V)
- Hook (0 = on-hook; 1 = off-hook)
- Ring (0 - Off; 1 - On)
- Line Connected (0 = Disconnected; 1 = Connected)
- Polarity state (0 = Normal; 1 = Reversed, 2 = N/A)
- Line polarity (0 = Positive; 1 = Negative)
- Message Waiting Indication (0 = Off; 1 = On)



**Note:** Use the Analog Line testing mechanism only for monitoring and never when there are calls in progress.

## Reader's Notes

## 56 Testing SIP Signaling Calls

A simulated endpoint can be configured on the device to test SIP signaling of calls between it and a remote destination. This feature is useful in that it can remotely verify SIP message flow without involving the remote end side in the debug process. The SIP test call simulates the SIP signaling process - call setup, SIP 1xx responses, and through to completing the SIP transaction with a 200 OK.

The test call sends Syslog messages to a Syslog server, showing the SIP message flow, DTMF signals, termination reasons, as well as voice quality statistics.

### 56.1 Configuring Test Call Endpoints

The Test Call table enables you to test the SIP signaling (setup and registration) of calls and media (DTMF signals) between a simulated phone on the device and a remote endpoint. These tests involve both incoming and outgoing calls, where the test endpoint can be configured as the caller or called party. Test calls can be dialed automatically at a user-defined interval and/or manually when required. The simulated phone and remote endpoints are defined as SIP URIs (user@host) and the remote destination can be defined as an IP Group, IP address, or according to an Outbound IP Routing rule. You can also enable automatic registration of the endpoint.

When a SIP test call is initiated, the device generates a SIP INVITE towards the remote endpoint (e.g., a SIP proxy server or softswitch). It simulates the SIP call setup process, managing SIP 1xx responses and completing the SIP transaction with a 200 OK.



#### Notes:

- By default, you can configure up to five test calls. This maximum can be increased by installing the relevant Software License Key. For more information, contact your AudioCodes sales representative.
- The Test Call Endpoint table can also be configured using the table ini file parameter Test\_Call (see 'SIP Test Call Parameters' on page 679) or CLI command, configure system > test-call > test-call-table.

#### ➤ To configure test calls:

1. Open the Test Call Table page (**Configuration** tab > **System** menu > **Test Call** > **Test Call Table**).
2. Click the **Add** button; the following dialog box appears:

**Figure 56-1: General Tab of Test Call Table**

Field	Value
Index	0
Endpoint URI	
Called URI	
Route By	GW Tel2IP
IP Group ID	-1
Destination Address	
Destination Transport Type	
SRD	0
Application Type	GW & IP2IP

3. Configure the test endpoint parameters as desired. See the table below for a

description of these parameters.

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

### Test Call Table Parameters

Parameter	Description
<b>General Tab</b>	
Endpoint URI [Test_Call_EndpointURI] CLI: endpoint-uri	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, this parameter is not configured.
Called URI [Test_Call_CalledURI] CLI: called-uri	Defines the destination (called) URI (user@host). The valid value is a string of up to 150 characters. By default, this parameter is not configured.
Route By [Test_Call_DestType] CLI: route-by	Defines the type of routing method. This applies to incoming and outgoing calls. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> GW Tel2IP = (Default) Calls are matched by (or routed to) an SRD and Application type (defined in the SRD and Application Type parameters below).</li> <li>▪ <b>[1]</b> IP Group = Calls are matched by (or routed to) an IP Group ID.</li> <li>▪ <b>[2]</b> Dest Address = Calls are matched by (or routed to) an SRD and application type.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ For REGISTER messages, the option <b>[0]</b> cannot be used as the routing method.</li> <li>▪ For REGISTER messages, if option <b>[1]</b> is used, only Server-type IP Groups can be used.</li> </ul>
IP Group ID [Test_Call_IPGroupID] CLI: ip-group-id	Defines the IP Group ID to which the test call is sent or from which it is received. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only if option <b>[1]</b> is configured for the 'Route By' parameter.</li> <li>▪ This IP Group is used for incoming and outgoing calls.</li> </ul>
Destination Address [Test_Call_DestAddress] CLI: dst-address	Defines the destination host. This can be defined as an IP address[:port] or DNS name[:port]. <b>Note:</b> This parameter is applicable only if the 'Route By' parameter is set to <b>[2]</b> (Dest Address).
Destination Transport Type [Test_Call_DestTransportType] CLI: dst-transport	Defines the transport type for outgoing calls. <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not configured (default)</li> <li>▪ <b>[0]</b> UDP</li> <li>▪ <b>[1]</b> TCP</li> <li>▪ <b>[2]</b> TLS</li> </ul> <b>Note:</b> This parameter is applicable only if the 'Route By' parameter is set to <b>[2]</b> (Dest Address).
SRD [Test_Call_SRD] CLI: srd	Defines the SRD for the endpoint. The default is SRD 0. <b>Note:</b> This parameter is applicable only if the 'Route By' parameter is set any option except <b>[1]</b> (IP Group).



Parameter	Description
Application Type <b>[Test_Call_ApplicationType]</b> CLI: application-type	Defines the application type for the endpoint. This, in effect, associates the IP Group and SRD to a specific SIP interface. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> GW &amp; IP2IP (default)</li> <li>▪ <b>[2]</b> SBC</li> </ul>
<b>Authentication Tab</b>	
<b>Note:</b> These parameters are applicable only if the test endpoint is set to <b>Caller</b> (see the 'Call Party' parameter).	
Auto Register <b>[Test_Call_AutoRegister]</b> CLI: auto-register	Enables automatic registration of the endpoint. The endpoint can register to the device itself or to the 'Destination Address' or 'IP Group ID' parameter settings (see above). <ul style="list-style-type: none"> <li>▪ <b>[0]</b> False (default)</li> <li>▪ <b>[1]</b> True</li> </ul>
User Name <b>[Test_Call_UserName]</b> CLI: user-name	Defines the authentication username. By default, no username is defined.
Password <b>[Test_Call_Password]</b> CLI: password	Defines the authentication password. By default, no password is defined.
<b>Test Settings Tab</b>	
Call Party <b>[Test_Call_CallParty]</b> CLI: call-party	Defines whether the test endpoint is the initiator or receiving side of the test call. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Caller (default)</li> <li>▪ <b>[1]</b> Called</li> </ul>
Maximum Channels for Session <b>[Test_Call_MaxChannels]</b> CLI: max-channels	Defines the maximum number of concurrent channels for the test session. For example, if you have configured an endpoint "101" and you set this parameter to "3", the device automatically creates three simulated endpoints - "101", "102" and "103" (i.e., consecutive endpoint URIs are assigned). The default is 1.
Call Duration <b>[Test_Call_CallDuration]</b> CLI: call-duration	Defines the call duration (in seconds). The valid value is -1 to 100000. The default is 20. A value of 0 means infinite. A value of -1 means that the parameter value is automatically calculated according to the values of the 'Calls per Second' and 'Maximum Channels for Session' parameters. <b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b> .
Calls per Second <b>[Test_Call_CallsPerSecond]</b> CLI: calls-per-second	Defines the number of calls per second. <b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b> .

Parameter	Description
Test Mode <b>[Test_Call_TestMode]</b> CLI: test-mode	<p>Defines the test session mode.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Once = (Default) The test runs until the lowest value between the following is reached: <ul style="list-style-type: none"> <li>✓ Maximum channels is reached for the test session, configured by 'Maximum Channels for Session'.</li> <li>✓ Call duration ('Call Duration') multiplied by calls per second ('Calls per Second').</li> <li>✓ Test duration expires, configured by 'Test Duration'.</li> </ul> </li> <li>▪ <b>[1]</b> Continuous = The test runs until the configured test duration is reached. If it reaches the maximum channels configured for the test session (in the 'Maximum Channels for Session'), it waits until the configured call duration of a currently established tested call expires before making the next test call. In this way, the test session stays within the configured maximum channels.</li> </ul> <p><b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b>.</p>
Test Duration <b>[Test_Call_TestDuration]</b> CLI: test-duration	<p>Defines the test duration (in minutes).</p> <p>The valid value is 0 to 100000. The default is 0 (i.e., unlimited).</p> <p><b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b>.</p>
Play <b>[Test_Call_Play]</b> CLI: play	<p>Enables playing a user-defined DTMF signal to the answered side of the call.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> DTMF</li> </ul> <p>To configure the played DTMF signal, see 'Configuring DTMF Tones for Test Calls' on page 648.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ 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' on page 163).</li> <li>▪ This parameter is applicable only if 'Call Party' is set to <b>Caller</b>.</li> </ul>
Schedule Interval <b>[Test_Call_ScheduleInterval]</b> CLI: schedule-interval	<p>Defines the interval (in minutes) between automatic outgoing test calls.</p> <p>The valid value range is 0 to 100000. The default is 0 (i.e., scheduling is disabled).</p> <p><b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b>.</p>

## 56.1.1 Starting, Stopping and Restarting Test Calls

The procedure below describes how to start, stop, and restart test calls.

### ➤ To start, stop, and restart a test call:

1. In the Test Call table, select the required test call entry; the **Actions** button appears above the table.
2. From the **Actions** drop-down list, choose the required command:
  - **Dial:** starts the test call (this action is applicable only if the test call party is the caller).
  - **Drop Call:** stops the test call.
  - **Restart:** ends all established calls and then starts the test call session again.

The status of the test call is displayed in the 'Test Status' field of the Test Call table:

- "Idle": test call is not active.
- "Scheduled": test call is planned to run (according to 'Schedule Interval' parameter settings)
- "Running": test call has been started (i.e., the **Dial** command was clicked)
- "Receiving": test call has been automatically activated by calls received for the test call endpoint from the remote endpoint (when all these calls end, the status returns to "Idle")
- "Terminating": test call is in the process of terminating the currently established calls (this occurs if the **Drop Call** command is clicked to stop the test)
- "Done": test call has been successfully completed (or was prematurely stopped by clicking the **Drop Call** command)

A more detailed description of this field is displayed below the table when you click the **Show/Hide** button (see 'Viewing Test Call Statistics' on page 647).

### 56.1.2 Viewing Test Call Statistics

In addition to viewing a brief status description of the test call in the 'Test Status' field (as described in 'Starting, Stopping and Restarting Test Calls' on page 646), you can also view a more detailed status description which includes test call statistics.

#### ➤ To view statistics of a test call:

1. Open the Test Call Table page (**Configuration** tab > **System** menu > **Test Call** > **Test Call Table**).
2. Select the test call table entry whose call statistics you want to view.
3. Click the **Show/Hide** button; the call statistics are displayed in the **Test Statistics** pane located below the table, as shown in the figure below:

Figure 56-2: Viewing Test Call Statistics

The screenshot shows the 'Test Call Table' with one entry in 'Running' status. Below the table, the 'Test Statistics' pane is expanded, showing the following information:

Test Call Table #0	
Endpoint URI: 101	Called URI: 102
Route By: GW Tel2IP	IP Group ID: -1
Destination Address: 10.13.4.12	Destination Transport Type: GW & IP2IP
SRD: 0	Application Type: GW & IP2IP
Auto Register: Disable	User Name: Caller
Password:	Call Party: Caller
Maximum Channels for Session: 4	Call Duration (seconds): 20
Calls per Second: 10	Test Mode: Once
Test Duration (minutes): 4	Play: DTMF
Schedule Interval (minutes): 0	

Test Statistics	
Elapsed Time [HH:MM:SS]: 00:00:11	Active Calls: 2
Call Attempts: 4	Total Established Calls: 2
Total Failed Attempts: 2	Remote Disconnections Count: 0
Test Status: Running	Average CPS:
Detailed Status: Running (Calls: 2, ASR: 50%)	

The 'Test Statistics' pane displays the following test session information:

- **Elapsed Time:** Duration of the test call since it was started (or restarted).
- **Active Calls:** The number of currently active test calls.
- **Call Attempts:** The number of calls that were attempted.
- **Total Established Calls:** The total number of calls that were successfully established.
- **Total Failed Attempts:** The total number of calls that failed to be established.

- **Remote Disconnections Count:** Number of calls that were disconnected by the remote side.
- **Average CPS:** The average calls per second.
- **Test Status:** Displays the status (brief description) as displayed in the 'Test Status' field (see 'Starting, Stopping and Restarting Test Calls' on page 646).
- **Detailed Status:** Displays a detailed description of the test call status::
  - "Idle": The test call is currently not active.
  - "Scheduled - Established Calls: <established calls>, ASR: <%>": The test call is planned to run (according to 'Schedule Interval' parameter settings) and also shows the following summary of completed test calls:
    - ◆ Total number of test calls that were established.
    - ◆ Number of successfully answered calls out of the total number of calls attempted (ASR).
  - "Running (Calls: <number of active calls>, ASR: <%>)": The test call has been started (i.e., the **Dial** command was clicked) and shows the following:
    - ◆ Number of currently active test calls.
    - ◆ Number of successfully answered calls out of the total number of calls attempted (Answer Seizure Ratio or ASR).
  - "Receiving (<number of active calls>)": The test call has been automatically activated by calls received for this configured test call endpoint from the configured remote endpoint. When all these calls terminate, the status returns to "Idle".
  - "Terminating (<number of active calls>)": The **Drop Call** command has been clicked to stop the test call and the test call is in the process of terminating the currently active test calls.
  - "Done - Established Calls: <established calls>, ASR: <%>": The test call has been successfully completed (or was prematurely stopped by clicking the **Drop Call** command) and shows the following:
    - ◆ Total number of test calls that were established.
    - ◆ Number of successfully answered calls out of the total number of calls attempted (ASR).



**Note:** On the receiving side, when the first call is accepted in "Idle" state, statistics are reset.

## 56.2 Configuring DTMF Tones for Test Calls

By default, no DTMF signal is played to an answered test call (incoming or outgoing). However, you can enable this per configured test call in the Test Call table (see 'Configuring Test Call Endpoints' on page 643). If enabled, the default DTMF signal that is played is "3212333". You can change this as described below.



### Notes:

- The DTMF signaling type (e.g., out-of-band or in-band) can be configured using the 'DTMF Transport Type' parameter. For more information, see 'Configuring DTMF Transport Types' on page 163.
- To generate DTMF tones, the device's DSP resources are required.

➤ **To configure the played DTMF signal to answered test call:**

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

**Figure 56-3: Test Call Settings Page**

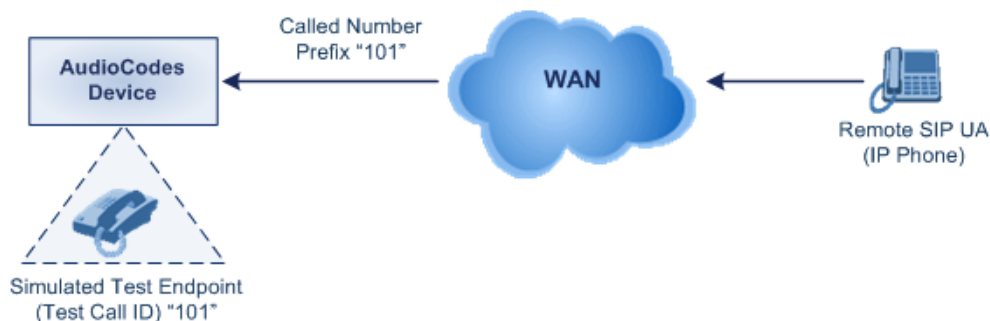
Test Call DTMF String	3212333
-----------------------	---------

2. In the 'Test Call DTMF String' field, enter the DTMF string (up to 15 digits).
3. Click **Submit**.

## 56.3 Configuring Basic Test Call

The Basic Test Call feature tests incoming Gateway / IP-to-IP calls from a remote SIP endpoint to a simulated test endpoint on the device. The only required configuration is to assign a prefix number (*test call ID*) to the simulated endpoint. All incoming calls with this called (destination) prefix number is identified as a test call and sent to the simulated endpoint. The figure below displays a basic test call example.

**Figure 56-4: Incoming Test Call Example**



➤ **To configure basic call testing:**

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

**Figure 56-5: Test Call Settings Page**

Test Call ID	<input type="text"/>
SBC Test ID	<input type="text"/>

2. In the 'Test Call ID' field, enter a prefix for the simulated endpoint.
3. Click **Submit** to apply your settings.



**Notes:**

- The Basic Test Call feature tests incoming calls only and is initiated only upon receipt of incoming calls with the configured prefix.
- For a full description of this parameter, see 'SIP Test Call Parameters' on page 679.
- This call test is done on all SIP interfaces.
- This call test is applicable only to the Gateway/IP-to-IP application.

## 56.4 Configuring SBC Test Call with External Proxy

The SBC Test Call feature tests incoming SBC SIP call flow between a simulated test endpoint on the device and a remote SIP endpoint, when registration and routing is done through an external proxy/registrar server such as a hosted IP PBX in the WAN. In other words, the complete SIP flow, including the path to/from the external proxy/registrar can be tested.

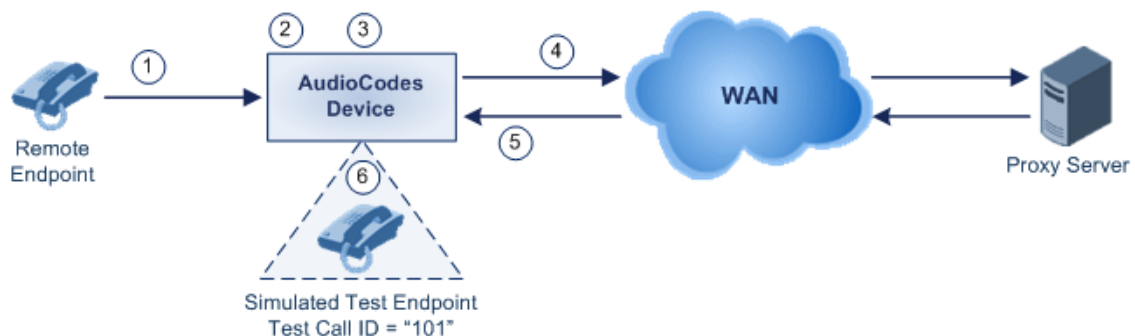
As this test call type involves an SBC call, you need to configure regular SBC rules such as classification and IP-to-IP routing. Therefore, this test call also allows you to verify correct SBC configuration.

For this test call, you also need to configure the following call IDs:

- Test Call ID - prefix number of the simulated endpoint on the device.
- SBC Test ID - prefix number of called number for identifying incoming call as SBC test call. The device removes this prefix, enabling it to route the call according to the IP-to-IP Routing rules to the external proxy/registrar, instead of directly to the simulated endpoint. Only when the device receives the call from the proxy/registrar, does it route the call to the simulated endpoint.

The figure below displays an example of an SBC test call:

**Figure 56-6: SBC Test Call Example**



1. The call is received from the remote endpoint with the called number prefix "8101".
2. As the 'SBC Test ID' parameter is set to "8", the device identifies this call as a test call and removes the digit "8" from the called number prefix, leaving it as "101".
3. The device performs the regular SBC processing such as classification and manipulation.
4. The device routes the call, according to the configured SBC IP-to-IP routing rules, to the proxy server.
5. The device receives the call from the proxy server.
6. As the 'Test Call ID' parameter is set to "101", the device identifies the incoming call as a test call and sends it directly to the simulated test endpoint "101".

➤ **To configure SBC call testing:**

1. Configure the test call parameters:
  - a. Open the Test Call Settings page (**Configuration** tab > **System** menu > **Test Call** > **Test Call Settings**).

**Figure 56-7: Test Call Settings Page**

Test Call ID	<input type="text"/>
SBC Test ID	<input type="text"/>

- b. In the 'Test Call ID' field, enter a prefix number for the simulated test endpoint on the device.
  - c. In the 'SBC Test ID' field, enter a called prefix number for identifying the call as an SBC test call.
  - d. Click **Submit** to apply your settings.
2. Configure regular SBC call processing rules for called number prefix "101", such as classification and IP-to-IP routing through a proxy server.



**Notes:**

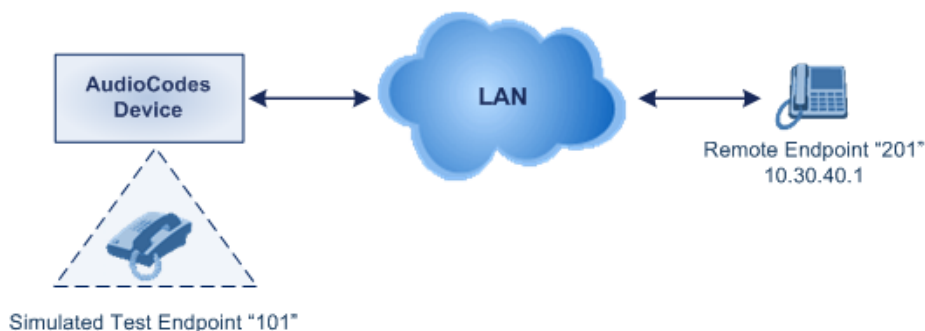
- For a full description of this parameter, see 'SIP Test Call Parameters' on page 679.
- This test call is initiated only upon receipt of incoming calls and with the configured prefix.
- This call test is done on all SIP interfaces.
- This test call is applicable only to the SBC application.

## 56.5 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 56-8: Single Test Call Example**



- Test Call table configuration:
  - ◆ Endpoint URI: "101"
  - ◆ Called URI: "201"
  - ◆ Route By: Dest Address



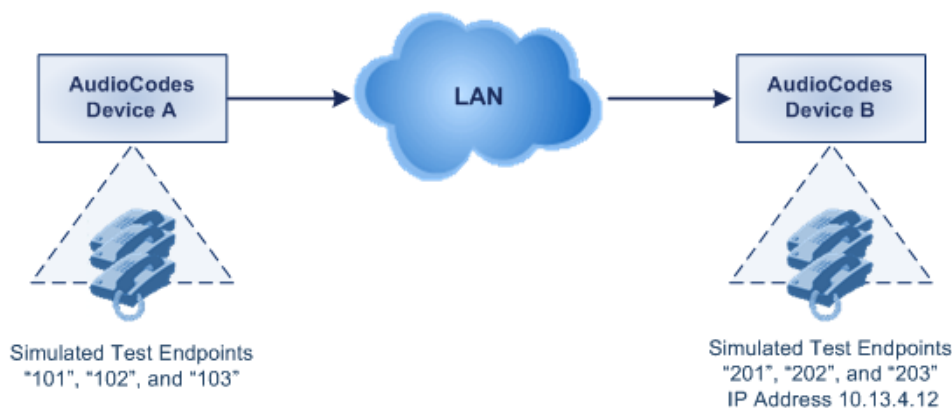
- ◆ Destination Address: "10.30.40.01"
- ◆ Call Party: Caller
- ◆ Test Mode: Once (default)

Alternatively, if you want to route the test call using the Outbound IP Routing table for the Gateway / IP-to-IP application, configure the following:

- Test Call table configuration:
  - ◆ Endpoint URI: 101@10.0.0.1
  - ◆ Route By: GW Tel2IP
  - ◆ Called URI: [201@10.30.40.1](#)
  - ◆ Call Party: Caller
- Outbound IP Routing table configuration:
  - ◆ Dest. Phone Prefix: 201 (i.e., the Called URI user-part)
  - ◆ Source Phone Prefix: 101 (i.e., the Endpoint URI user-part)
  - ◆ Dest. IP Address: 10.30.40.1

- **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 56-9: Batch Test Call Example**



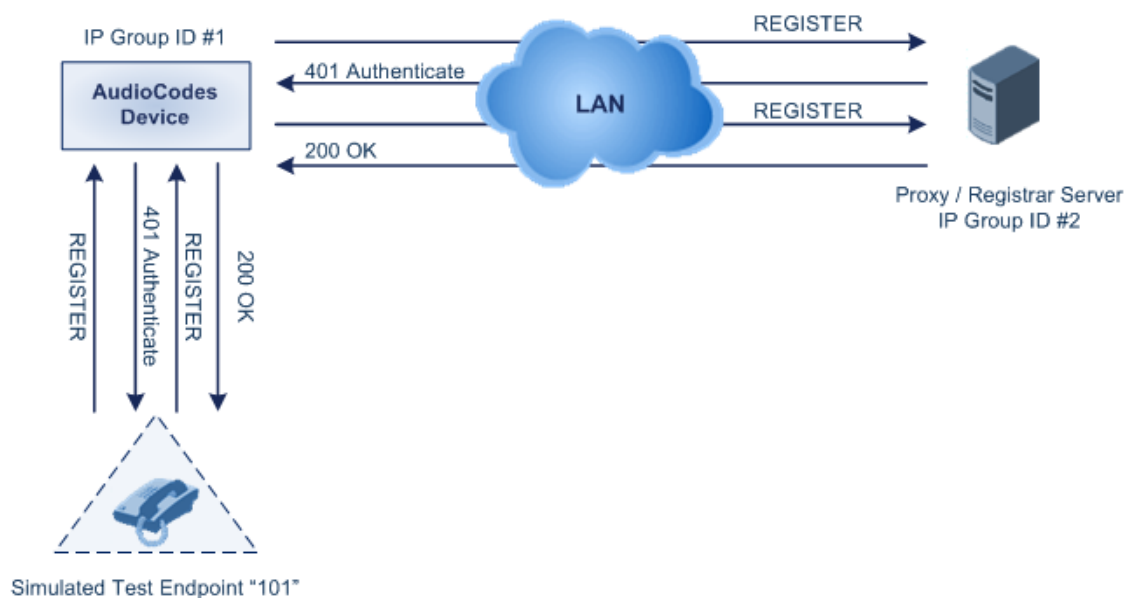
- Test Call table configuration at Device A:
  - ◆ Endpoint URI: "101"
  - ◆ Called URI: "201"
  - ◆ Route By: Dest Address
  - ◆ Destination Address: "10.13.4.12"
  - ◆ Call Party: Caller
  - ◆ Maximum Channels for Session: "3" (this setting configures three endpoints - "101", "102" and "103")
  - ◆ Call Duration: "5" (seconds)
  - ◆ Calls per Sec: "1"
  - ◆ Test Mode: Continuous
  - ◆ Test Duration: "3" (minutes)
  - ◆ Schedule Interval: "180" (minutes)



- Test Call table configuration at Device B:
  - ◆ Endpoint URI: "201"
  - ◆ Call Party: Caller
  - ◆ Maximum Channels for Session: "3" (this setting configures three endpoints - "201", "202" and "203")

- **Registration Test Call Scenario:** This example describes the configuration for testing the registration and authentication (i.e., username and password) process of a simulated test endpoint on the device with an external proxy/registrar server. This is useful, for example, for verifying that endpoints located in the LAN can register with an external proxy and subsequently, communicate with one another.

**Figure 56-10: Test Call Registration Example**



This example assumes that you have configured your device for communication between LAN phone users such as IP Groups to represent the device (10.13.4.12) and the proxy server, and IP-to-IP routing rules to route calls between these IP Groups.

- Test Call table configuration:
  - ◆ Endpoint URI: "101"
  - ◆ Called URI: "itsp"
  - ◆ Route By: Dest Address
  - ◆ Destination Address: "10.13.4.12" (this is the IP address of the device itself)
  - ◆ Auto Register: Enable
  - ◆ User Name: "testuser"
  - ◆ Password: "12345"
  - ◆ Call Party: Caller

## Reader's Notes

## 57 Running Data-Router Diagnostic Tests

The **Diagnostics** item can assist you in testing network connectivity and viewing statistics such as the number of packets transmitted and received, round-trip time and success status. This page allows you to run network connectivity tests (ping), query the physical address (MAC) of a host, and run a trace route test.

➤ **To run diagnostic tests:**

1. Click the **Diagnostics** item (**Status & Diagnostics** tab > **Data Status** menu > **Diagnostics**); the following page appears:

**Figure 57-1: System - Diagnostics Page**

The screenshot displays the 'System - Diagnostics Page' with three distinct sections for network testing:

- Ping (ICMP Echo):** Includes a 'Destination' text input field, a 'Number of pings' input field with the value '4', and a 'Status' label. A 'Go' button is located to the right of the input fields.
- ARP:** Includes a 'Destination' input field divided into four segments, each containing a '0'. A 'Status' label and a 'Go' button are also present.
- Traceroute:** Includes a 'Destination' text input field and a 'Status' label. A 'Go' button is located to the right of the input field.

2. To diagnose network connectivity, under the 'Ping (ICMP Echo)' group, perform the following:
  - a. In the 'Destination' field, enter the IP address or URL to be tested.
  - b. In the 'Number of Pings' field, enter the number of pings you would like to run.
  - c. Click **Go**; in a few moments, diagnostic statistics are displayed. If no new information appears, click **Refresh**.
3. To query the physical address (MAC) of a host, under the 'ARP' group, perform the following:
  - a. In the 'Destination' field, enter an IP address of the target host.
  - b. Click **Go**; in a few moments, diagnostic statistics are displayed. If no new information is displayed, click **Refresh**.
4. To run a traceroute test, under the Traceroute group, perform the following:
  - a. In the 'Destination' field, enter the IP address or URL to be tested.
  - b. Click **Go**; the traceroute test commences, constantly refreshing the page.
  - c. To stop the test and view the results, click **Cancel**.

## Reader's Notes

# Part XIV

## Appendix



## 58 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.

### Dialing Plan Notations for Prefixes and Suffixes

Notation	Description
<b>x</b> (letter "x")	Denotes any single digit.
<b>#</b> (pound symbol)	<ul style="list-style-type: none"> <li>When used at the end of a prefix, it denotes the end of a number. For example, <b>54324xx#</b> represents a 7-digit number that starts with the digits 54324.</li> <li>When used anywhere in the suffix, it is part of the number. For example, <b>(3#45)</b> can represent the number string, 123#45.</li> </ul>
<b>*</b> (asterisk symbol)	<ul style="list-style-type: none"> <li>When used in the prefix, it denotes any number.</li> <li>When used in the suffix, it is part of the number. For example, <b>(3*45)</b> can represent the number string, 123*45.</li> </ul>
<b>\$</b> (dollar sign)	<p>Denotes an empty prefix for incoming IP calls that do not have a user part in the Request-URI, or for incoming Tel calls that do not have a called or calling number. This is used for the following matching criteria:</p> <ul style="list-style-type: none"> <li>Source and Destination Phone Prefix</li> <li>Source and Destination Username</li> <li>Source and Destination Calling Name Prefix</li> </ul>

#### Range of Digits

##### Notes:

- 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])**.

<b>[n-m]</b> or <b>(n-m)</b>	<p>Represents a range of numbers, for example:</p> <ul style="list-style-type: none"> <li>To depict numbers from 5551200 to 5551300: <ul style="list-style-type: none"> <li>✓ Prefix: <b>[5551200-5551300]#</b></li> <li>✓ Suffix: <b>(5551200-5551300)</b></li> </ul> </li> <li>To depict numbers from 123100 to 123200: <ul style="list-style-type: none"> <li>✓ Prefix: <b>123[100-200]</b></li> <li>✓ Suffix: <b>(123[100-200])</b></li> </ul> </li> <li>To depict prefix and suffix numbers together: <ul style="list-style-type: none"> <li>✓ 03(100): for any number that starts with 03 and ends with 100.</li> <li>✓ <b>[100-199](100,101,105)</b>: for a number that starts with 100 to 199 and ends with 100, 101 or 105.</li> <li>✓ 03(abc): for any number that starts with 03 and ends with abc.</li> <li>✓ 03(5xx): for any number that starts with 03 and ends with 5xx.</li> <li>✓ 03(400,401,405): for any number that starts with 03 and ends with 400 or 401 or 405.</li> </ul> </li> </ul>
------------------------------	---

Notation	Description
	<b>Notes:</b> <ul style="list-style-type: none"> <li>The value <math>n</math> must be less than the value <math>m</math>.</li> <li>Only numerical ranges are supported (not alphabetical letters).</li> <li>For suffix ranges, the starting (<math>n</math>) and ending (<math>m</math>) numbers in the range must have the same number of digits. For example, (23-34) is correct, but (3-12) is not.</li> </ul>
[ $n,m,\dots$ ] or ( $n,m,\dots$ )	<p>Represents multiple numbers. For example, to depict a one-digit number starting with 2, 3, 4, 5, or 6:</p> <ul style="list-style-type: none"> <li>Prefix: <b>[2,3,4,5,6]#</b></li> <li>Suffix: <b>(2,3,4,5,6)</b></li> <li>Prefix with Suffix: <b>[2,3,4,5,6](8,7,6)</b> - prefix is denoted in square brackets; suffix in parenthesis</li> </ul> <p>For <b>prefix only</b>, the notations <math>d[n,m]e</math> and <math>d[n-m]e</math> can also be used:</p> <ul style="list-style-type: none"> <li>To depict a five-digit number that starts with 11, 22, or 33: <b>[11,22,33]xxx#</b></li> <li>To depict a six-digit number that starts with 111 or 222: <b>[111,222]xxx#</b></li> </ul> <p><b>Note:</b> Up to three digits can be used to denote each number.</p>
[ $n1-m1,n2-m2,a,b,c,n3-m3$ ] or ( $n1-m1,n2-m2,a,b,c,n3-m3$ )	<p>Represents a mixed notation of single numbers and multiple ranges. For example, to depict numbers 123 to 130, 455, 766, and 780 to 790:</p> <ul style="list-style-type: none"> <li>Prefix: <b>[123-130,455,766,780-790]</b></li> <li>Suffix: <b>(123-130,455,766,780-790)</b></li> </ul> <p><b>Note:</b> The ranges and the single numbers used in the dial plan must have the same number of digits. For example, each number range and single number in the dialing plan example above consists of three digits.</p>



**Note:** When configuring phone numbers or prefixes in the Web interface, enter them only as digits without any other characters. For example, if you wish to enter the phone number 555-1212, it must be entered as 5551212 without the hyphen (-). If the hyphen is entered, the entry is invalid.



## 59 Configuration Parameters Reference

The device's VoIP functionality (not data-routing functionality) configuration parameters, default values, and their descriptions are documented in this section.



**Notes:** Parameters and values enclosed in square brackets [...] represent the *ini* file parameters and their enumeration values.

### 59.1 Networking Parameters

This subsection describes the device's networking parameters.

#### 59.1.1 Multiple VoIP Network Interfaces and VLAN Parameters

The IP network interfaces and VLAN parameters are described in the table below.

**IP Network Interfaces and VLAN Parameters**

Parameter	Description
<b>Multiple Interface Table</b>	
Web: Multiple Interface Table EMS: IP Interface Settings CLI: configure voip > interface network-if display <b>[InterfaceTable]</b>	<p>This table parameter configures the Multiple Interface table. The format of this parameter is as follows:</p> <p><b>[InterfaceTable]</b>            FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID, InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress, InterfaceTable_SecondaryDNSServerIPAddress, InterfaceTable_UnderlyingInterface;  <b>[InterfaceTable]</b></p> <p>For example:            InterfaceTable 0 = 0, 0, 192.168.85.14, 16, 0.0.0.0, 1, Management;            InterfaceTable 1 = 2, 0, 200.200.85.14, 24, 0.0.0.0, 200, Control;            InterfaceTable 2 = 1, 0, 211.211.85.14, 24, 211.211.85.1, 211, Media;</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a description of this parameter, see 'Configuring IP Network Interfaces' on page 107.</li> </ul>
<b>VLAN Parameters</b>	
<b>[EnableNTPasOAM]</b>	<p>Defines the application type for Network Time Protocol (NTP) services.</p> <ul style="list-style-type: none"> <li><b>[1]</b> = OAMP (default)</li> <li><b>[0]</b> = Control</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>

## 59.1.2 Routing Parameters

The IP network routing parameters are described in the table below.

**IP Network Routing Parameters**

Parameter	Description
<b>Static IP Routing Table</b>	
Web/EMS: IP Routing Table CLI: configure voip > static <b>[StaticRouteTable]</b>	<p>Defines up to 30 static VoIP IP routing rules for the device. These rules can be associated with IP interfaces defined in the Multiple Interface table (InterfaceTable parameter). The routing decision for sending the outgoing IP packet is based on the source subnet/VLAN. If not associated with an IP interface, the static IP rule is based on destination IP address.</p> <p>When the destination of an outgoing IP packet does not match one of the subnets defined in the Multiple Interface table, the device searches this table for an entry that matches the requested destination host/network. If such an entry is found, the device sends the packet to the indicated router (i.e., next hop). If no explicit entry is found, the packet is sent to the default gateway according to the source interface of the packet (if defined).</p> <p>The format of this parameter is as follows:</p> <p><b>[ StaticRouteTable ]</b>  FORMAT StaticRouteTable_Index = StaticRouteTable_InterfaceName, StaticRouteTable_Destination, StaticRouteTable_PrefixLength, StaticRouteTable_Gateway, StaticRouteTable_Description;  <b>[ \StaticRouteTable ]</b></p> <p><b>Note:</b> For a description of this parameter, see 'Configuring Static IP Routing' on page <a href="#">115</a>.</p>

## 59.1.3 Quality of Service Parameters

The Quality of Service (QoS) parameters are described in the table below.

**QoS Parameters**

Parameter	Description
<b>Layer-2 Class Of Service (CoS) Parameters (VLAN Tag Priority Field)</b>	
Web: DiffServ Table EMS: QoS Settings – DSCP to QoS Mapping CLI: configure voip > vlan-mapping <b>[DiffServToVlanPriority]</b>	<p>This table parameter configures DiffServ-to-VLAN Priority mapping. For each packet sent to the LAN, the VLAN Priority of the packet is set according to the DiffServ value in the IP header of the packet. The format of this ini file is as follows:</p> <p><b>[ DiffServToVlanPriority ]</b>  FORMAT DiffServToVlanPriority_Index = DiffServToVlanPriority_DiffServ, DiffServToVlanPriority_VlanPriority;  <b>[ \DiffServToVlanPriority ]</b></p> <p>For example:  DiffServToVlanPriority 0 = 46, 6;  DiffServToVlanPriority 1 = 40, 6;  DiffServToVlanPriority 2 = 26, 4;  DiffServToVlanPriority 3 = 10, 2;</p> <p><b>Notes:</b></p>

Parameter	Description
	<ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a description of this table, see Configuring Quality of Service on page 118</li> </ul>
<b>Layer-3 Class of Service (TOS/DiffServ) Parameters</b>	
Web: Media Premium QoS EMS: Premium Service Class Media Diff Serv CLI: media-qos <b>[PremiumServiceClassMediaDiffServ]</b>	Defines the DiffServ value for Premium Media CoS content. The valid range is 0 to 63. The default is 46. <b>Note:</b> The value for the Premium Control DiffServ is determined by the following (according to priority): <ul style="list-style-type: none"> <li>IPDiffServ value in the selected IP Profile (IPProfile parameter).</li> <li>PremiumServiceClassMediaDiffServ.</li> </ul>
Web: Control Premium QoS EMS: Premium Service Class Control Diff Serv CLI: control-qos <b>[PremiumServiceClassControlDiffServ]</b>	Defines the DiffServ value for Premium Control CoS content (Call Control applications). The valid range is 0 to 63. The default is 40. <b>Notes:</b> <ul style="list-style-type: none"> <li>The value for the Premium Control DiffServ is determined by the following (according to priority):               <ul style="list-style-type: none"> <li>✓ SigIPDiffserv value in the selected IP Profile (IPProfile parameter).</li> <li>✓ PremiumServiceClassControlDiffServ.</li> </ul> </li> </ul>
Web: Gold QoS EMS: Gold Service Class Diff Serv CLI: gold-qos <b>[GoldServiceClassDiffServ]</b>	Defines the DiffServ value for the Gold CoS content (Streaming applications). The valid range is 0 to 63. The default is 26.
Web: Bronze QoS EMS: Bronze Service Class Diff Serv CLI: bronze-qos <b>[BronzeServiceClassDiffServ]</b>	Defines the DiffServ value for the Bronze CoS content (OAMP applications). The valid range is 0 to 63. The default is 10.

### 59.1.4 NAT and STUN Parameters

The Network Address Translation (NAT) parameters are described in the table below.

#### NAT Parameters

Parameter	Description
<b>NAT Parameters</b>	
Web/EMS: NAT Traversal CLI: disable-NAT-traversal <b>[DisableNAT]</b>	Enables the NAT mechanism. For more information, see 'First Incoming Packet Mechanism' on page 129. <ul style="list-style-type: none"> <li><b>[0]</b> Enable</li> <li><b>[1]</b> Disable (default)</li> </ul>
Web: NAT IP Address EMS: Static NAT IP Address CLI: nat-ip-addr	Defines the global (public) IP address of the device to enable static NAT between the device and the Internet. <b>Note:</b> For this parameter to take effect, a device reset is required.

Parameter	Description
<b>[StaticNatIP]</b>	
Web/EMS: Inbound Media Latch Mode CLI: inbound-media-latch-mode <b>[InboundMediaLatchMode]</b>	<p>Enables the receipt of media streams whose IP address/port are not configured for the channel.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Strict = Accepts only the media stream configured for the channel.</li> <li>▪ <b>[1]</b> Dynamic = (Default) Accepts any media stream.</li> </ul>

## 59.1.5 NFS Parameters

The Network File Systems (NFS) configuration parameters are described in the table below.

**NFS Parameters**

Parameter	Description
CLI: base-port <b>[NFSBasePort]</b>	<p>Defines the start of the range of numbers used for local UDP ports used by the NFS client. The maximum number of local ports is maximum channels plus maximum NFS servers.</p> <p>The valid range is 0 to 65535. The default is 47000.</p>
<b>NFS Table</b>	
Web: NFS Table EMS: NFS Settings <b>[NFSServers]</b>	<p>This table parameter defines up to 16 NFS file systems so that the device can access a remote server's shared files and directories for loading cmp, ini, and auxiliary files (using the Automatic Update mechanism).</p> <p>The format of this table ini file parameter is as follows:</p> <p><b>[NFSServers]</b>  FORMAT NFSServers_Index = NFSServers_HostOrIP,  NFSServers_RootPath, NFSServers_NfsVersion,  NFSServers_AuthType, NFSServers_UID, NFSServers_GID,  NFSServers_VlanType;  <b>[NFSServers]</b></p> <p>For example:  NFSServers 1 = 101.1.13, /audio1, 3, 1, 0, 1, 1;</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring NFS Settings' on page 123.</p>

## 59.1.6 DNS Parameters

The Domain name System (DNS) parameters are described in the table below.

**DNS Parameters**

Parameter	Description
<b>Internal DNS Table</b>	
Web: Internal DNS Table EMS: DNS Information CLI: configure voip > control-network dns Dns2Ip <b>[DNS2IP]</b>	<p>This table parameter defines the internal DNS table for resolving host names into IP addresses. Up to four different IP addresses (in dotted-decimal notation) can be assigned to a host name.</p> <p>The format of this parameter is as follows:</p> <p><b>[Dns2Ip]</b>            FORMAT Dns2Ip_Index = Dns2Ip_DomainName,            Dns2Ip_FirstIpAddress, Dns2Ip_SecondIpAddress,            Dns2Ip_ThirdIpAddress, Dns2Ip_FourthIpAddress;  <b>[Dns2Ip]</b></p> <p>For example:            Dns2Ip 0 = DnsName, 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4;</p> <p><b>Note:</b> For a detailed description of this table parameter, see 'Configuring the Internal DNS Table' on page <a href="#">120</a>.</p>
<b>Internal SRV Table</b>	
Web: Internal SRV Table EMS: DNS Information CLI: configure voip > control-network dns Srv2Ip <b>[SRV2IP]</b>	<p>This table parameter defines the internal SRV table for resolving host names into DNS A-Records. Three different A-Records can be assigned to a host name. Each A-Record contains the host name, priority, weight, and port. The format of this parameter is as follows:</p> <p><b>[SRV2IP]</b>            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;  <b>[SRV2IP]</b></p> <p>For example:            SRV2IP 0 =            SrvDomain,0,Dnsname1,1,1,500,Dnsname2,2,2,501,\$\$,0,0,0;</p> <p><b>Note:</b> For a detailed description of this table parameter, see 'Configuring the Internal SRV Table' on page <a href="#">121</a>.</p>

## 59.1.7 DHCP Parameters

The Dynamic Host Control Protocol (DHCP) parameters are described in the table below.

**DHCP Parameters**

Parameter	Description
Web: Enable DHCP EMS: DHCP Enable <b>[DHCPEnable]</b>	<p>Enables Dynamic Host Control Protocol (DHCP) functionality.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p>

Parameter	Description
	<ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>After you enable the DHCP server, do the following: <ul style="list-style-type: none"> <li>d. Enable DHCP and save the configuration.</li> <li>e. Perform a cold reset using the device's hardware reset button (soft reset using the Web interface doesn't trigger the DHCP procedure and this parameter reverts to 'Disable').</li> </ul> </li> <li>This parameter is a special 'Hidden' parameter. Once defined and saved in flash memory, its assigned value doesn't revert to its default even if the parameter doesn't appear in the <i>ini</i> file.</li> </ul>
EMS: DHCP Speed Factor <b>[DHCPSpeedFactor]</b>	<p>Defines the DHCP renewal speed.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable</li> <li><b>[1]</b> = (Default) Normal</li> <li><b>[2]</b> to <b>[10]</b> = Fast</li> </ul> <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><b>Note:</b> For this parameter to take effect, a device reset is required.</p>

## 59.1.8 NTP and Daylight Saving Time Parameters

The Network Time Protocol (NTP) and daylight saving time parameters are described in the table below.

**NTP and Daylight Saving Time Parameters**

Parameter	Description
<b>NTP Parameters</b> <b>Note:</b> For more information on Network Time Protocol (NTP), see 'Simple Network Time Protocol Support' on page 101.	
Web: NTP Server DN/IP EMS: Server IP Address CLI: primary-server <b>[NTPServerIP]</b>	<p>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.</p> <p>The default IP address is 0.0.0.0 (i.e., internal NTP client is disabled).</p>
Web: NTP Secondary Server IP <b>[NTPSecondaryServerIP]</b>	<p>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.</p> <p>The default IP address is 0.0.0.0.</p>
Web: NTP UTC Offset EMS: UTC Offset CLI: utc-offset <b>[NTPServerUTCOffset]</b>	<p>Defines the Universal Time Coordinate (UTC) offset (in seconds) from the NTP server.</p> <p>The default offset is 0. The offset range is -43200 to 43200.</p>
Web: NTP Update Interval EMS: Update Interval CLI: update-interval <b>[NTPUpdateInterval]</b>	<p>Defines the time interval (in seconds) that the NTP client requests for a time update.</p> <p>The default interval is 86400 (i.e., 24 hours). The range is 0 to 214783647.</p> <p><b>Note:</b> It is not recommend to set this parameter to beyond one month (i.e., 2592000 seconds).</p>

Parameter	Description
<b>Daylight Saving Time Parameters</b>	
Web: Day Light Saving Time EMS: Mode CLI: summer-time <b>[DayLightSavingTimeEnable]</b>	Enables daylight saving time. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Web: Start Time or Day of Month Start EMS: Start CLI: start <b>[DayLightSavingTimeStart]</b>	Defines the date and time when daylight saving begins. This value can be configured using any of the following formats: <ul style="list-style-type: none"> <li>▪ Day of year - <i>mm:dd:hh:mm</i>, where: <ul style="list-style-type: none"> <li>✓ <i>mm</i> denotes month</li> <li>✓ <i>dd</i> denotes date of the month</li> <li>✓ <i>hh</i> denotes hour</li> <li>✓ <i>mm</i> denotes minutes</li> </ul> For example, "05:01:08:00" denotes daylight saving starting from May 1 at 8 A.M.</li> <li>▪ Day of month - <i>mm:day/wk:hh:mm</i>, where: <ul style="list-style-type: none"> <li>✓ <i>mm</i> denotes month (e.g., 04)</li> <li>✓ <i>day</i> denotes day of week (e.g., FRI)</li> <li>✓ <i>wk</i> denotes week of the month (e.g., 03)</li> <li>✓ <i>hh</i> denotes hour (e.g., 23)</li> <li>✓ <i>mm</i> denotes minutes (e.g., 10)</li> </ul> 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.</li> </ul>
Web: End Time or Day of Month End EMS: End CLI: end <b>[DayLightSavingTimeEnd]</b>	Defines the date and time when daylight saving ends. For a description of the format of this value, see the DayLightSavingTimeStart parameter.
Web/EMS: Offset CLI: offset <b>[DayLightSavingTimeOffset]</b>	Defines the daylight saving time offset (in minutes). The valid range is 0 to 120. The default is 60.

### 59.1.9 Power over Ethernet Parameters

The power-over-Ethernet (PoE) parameters are described in the table below.

#### PoE Parameters

Parameter	Description
Web: Power over Ethernet Settings CLI: configure system > interface poe-table <b>[POETable]</b>	This table enables PoE (IEEE 802.3af-2003) per LAN port and configures the maximum power consumption allowed per port for Class 0 clients connected to it. <b>[POETable]</b> FORMAT POETable_Index = POETable_PortEnable, POETable_PortPower, POETable_PortATEnable;

Parameter	Description
	<p>[ \POETable ]</p> <p>Where:</p> <ul style="list-style-type: none"> <li>Index = Port number (where 0 is Port 1)</li> <li>PortEnable = enables <b>[1]</b> or disables <b>[0]</b> IEEE 802.3af-2003 PoE</li> <li>PortPower = defines maximum power consumption</li> </ul> <p><b>Note:</b> For a description of this parameter, see 'Configuring Power over Ethernet' on page <a href="#">103</a>.</p>

## 59.2 Management Parameters

This subsection describes the device's Web and Telnet parameters.

### 59.2.1 General Parameters

The general management parameters are described in the table below.

**General Management Parameters**

Parameter	Description
WAN OAMP Interface CLI: bind GigabitEthernet <slot/port.vlanId> oamp <b>[OAMPWanInterfaceName]</b>	Binds the OAMP interface to a WAN interface, which can later be associated with a Virtual Routing and Forwarding (VRF).
Web: Allow WAN access to HTTP CLI: wan-http-allow <b>[AllowWanHTTP]</b>	Enables WAN access to the management interface through HTTP. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Allow WAN access to HTTPS CLI: wan-https-allow <b>[AllowWanHTTPS]</b>	Enables WAN access to the management interface through HTTPS. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Allow WAN access to SNMP CLI: wan-snmp-allow <b>[AllowWanSNMP]</b>	Enables WAN access to the management interface through SNMP. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>Web: Allow WAN access to Telnet</b> CLI: wan-telnet-allow <b>[AllowWanTelnet]</b>	Enables WAN access to the management interface through Telnet. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Allow WAN access to SSH CLI: wan-ssh-allow <b>[AllowWanSSH]</b>	Enables WAN access to the management interface through SSH. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>



Parameter	Description
Web: Web and Telnet Access List Table EMS: Web Access Addresses <b>[WebAccessList_x]</b>	<p>This table configures up to ten IP addresses that are permitted to access the device's Web interface and Telnet interfaces. Access from an undefined IP address is denied. When no IP addresses are defined in this table, this security feature is inactive (i.e., the device can be accessed from any IP address).</p> <p>The default is 0.0.0.0 (i.e., the device can be accessed from any IP address).</p> <p>For example: WebAccessList_0 = 10.13.2.66 WebAccessList_1 = 10.13.77.7</p> <p>For a description of this parameter, see 'Configuring Web and Telnet Access List' on page 67.</p>

## 59.2.2 Web Parameters

The Web parameters are described in the table below.

### Web Parameters

Parameter	Description
Web: Password Change Interval <b>[WebUserPassChangeInterval]</b>	<p>Defines the duration (in minutes) of the validity of Web login passwords. When this duration expires, the password of the Web user must be changed.</p> <p>The valid value is 0 to 100000, where 0 means that the password is always valid. The default is 1140.</p> <p><b>Note:</b> This parameter is applicable only when using the Web Users table, where the default value of the 'Password Age' parameter in the Web Users table inherits this parameter's value.</p>
Web: User inactivity timer <b>[UserInactivityTimer]</b>	<p>Defines the duration (in days) for which a user has not logged in to the Web interface, after which the status of the user becomes inactive and can no longer access the Web interface. These users can only log in to the Web interface if their status is changed (to New or Valid) by a System Administrator or Master user.</p> <p>The valid value is 0 to 10000, where 0 means inactive. The default is 90.</p> <p><b>Note:</b> This parameter is applicable only when using the Web Users table.</p>
Web: Session Timeout <b>[WebSessionTimeout]</b>	<p>Defines the duration (in minutes) of Web inactivity of a logged-in user, after which the user is automatically logged off the Web interface.</p> <p>The valid value is 0-100000, where 0 means no timeout. The default is 15.</p> <p><b>Note:</b> This parameter can apply to all users, or per user when set in the Web Users table.</p>
Web: Deny Access On Fail Count <b>[DenyAccessOnFailCount]</b>	<p>Defines the maximum number of failed login attempts, after which the requesting IP address is blocked.</p> <p>The valid value range is 0 to 10. The values 0 and 1 mean immediate block. The default is 3.</p>

Parameter	Description
Web: Deny Authentication Timer EMS: WEB Deny Authentication Timer <b>[DenyAuthenticationTimer]</b>	<p>Defines the duration (in seconds) for which login to the Web interface is denied from a specific IP address (for all users) when the number of failed login attempts has exceeded the maximum. This maximum is defined by the DenyAccessOnFailCount parameter. Only after this time expires can users attempt to login from this same IP address.</p> <p>The valid value is 0 to 100000, where 0 means that login is not denied regardless of number of failed login attempts. The default is 60.</p>
Web: Display Login Information <b>[DisplayLoginInformation]</b>	<p>Enables display of user's login information on each successful login attempt.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul>
<b>[EnableMgmtTwoFactorAuthentication]</b>	<p>Enables Web login authentication using a third-party, smart card.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul> <p>When enabled, the device retrieves the Web user's login username from the smart card, which is automatically displayed (read-only) in 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>
EMS: HTTPS Port CLI: http-port <b>[HTTPport]</b>	<p>Defines the LAN HTTP port for Web management (default is 80). To enable Web management from the LAN, configure the desired port.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: Disable WEB Config <b>[DisableWebConfig]</b>	<p>Determines whether the entire Web interface is read-only.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Enables modifications of parameters.</li> <li><b>[1]</b> = Web interface is read-only.</li> </ul> <p>When in read-only mode, parameters can't be modified. In addition, the following pages can't be accessed: 'Web User Accounts', 'Certificates', 'Regional Settings', 'Maintenance Actions' and all file-loading pages ('Load Auxiliary Files', 'Software Upgrade Wizard', and 'Configuration File').</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> </ul>
<b>[ResetWebPassword]</b>	<p>Resets the username and password of the primary ("Admin") and secondary ("User") accounts to their default settings ("Admin" and "Admin" respectively), and deletes all other users that may have been configured.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Password and username retain their values.</li> <li><b>[1]</b> = Password and username are reset.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>You cannot reset the username and password through the Web interface (by loading an ini file or on the AdminPage). To reset the username and password, use SNMP: <ul style="list-style-type: none"> <li>a. Set acSysGenericNILine to WEBPasswordControlViaSNMP = 1, and reset the device with a flash burn (set</li> </ul> </li> </ul>

Parameter	Description
	<p>acSysActionSetResetControl to 1 and acSysActionSetReset to 1).</p> <p><b>b.</b> Change the username and password in the acSysWEBAccessEntry table. Use the following format:            Username acSysWEBAccessUserName: old/pass/new            Password acSysWEBAccessUserCode: username/old/new</p>
<b>[WelcomeMessage]</b>	<p>Enables and defines a Welcome message that appears on the Web Login page for logging in to the Web interface.            The format of this parameter is as follows:</p> <p><b>[WelcomeMessage]</b>            FORMAT WelcomeMessage_Index = WelcomeMessage_Text  <b>[WelcomeMessage]</b></p> <p>For Example:            FORMAT WelcomeMessage_Index = WelcomeMessage_Text            WelcomeMessage 1 = "*****";            WelcomeMessage 2 = "***** This is a Welcome message *****";            WelcomeMessage 3 = "*****";</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Each index row represents a line of text in the Welcome message box. Up to 20 lines (or rows) of text can be defined.</li> <li>The configured text message must be enclosed in double quotation marks (i.e., "...").</li> <li>If this parameter is not configured, no Welcome message is displayed.</li> </ul>

### 59.2.3 Telnet Parameters

The Telnet parameters are described in the table below. Note: Telnet is currently supported only for debugging from the LAN interface.

**Telnet Parameters**

Parameter	Description
Web: Embedded Telnet Server EMS: Server Enable CLI: telnet <b>[TelnetServerEnable]</b>	<p>Enables the device's embedded Telnet server. Telnet is disabled by default for security.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable Unsecured</li> <li><b>[2]</b> Enable Secured (SSL)</li> </ul> <p><b>Note:</b> Only the primary Web User Account (which has Security Administration access level) can access the device using Telnet (see 'Configuring Web User Accounts' on page 58).</p>
Web: Telnet Server TCP Port EMS: Server Port CLI: telnet-port <b>[TelnetServerPort]</b>	<p>Defines the port number for the embedded Telnet server.            The valid range is all valid port numbers. The default port is 23.</p>
Web: Telnet Server Idle Timeout EMS: Server Idle	<p>Defines the timeout (in minutes) for disconnection of an idle Telnet session. When set to zero, idle sessions are not disconnected.</p>

Parameter	Description
Disconnect CLI: idle-timeout [TelnetServerIdleDisconnect]	The valid range is any value. The default is 0. <b>Note:</b> For this parameter to take effect, a device reset is required.

## 59.2.4 SNMP Parameters

The SNMP parameters are described in the table below.

**SNMP Parameters**

Parameter	Description
Web: Enable SNMP CLI: disable [DisableSNMP]	Enables SNMP. <ul style="list-style-type: none"> <li>[0] Enable = (Default) SNMP is enabled.</li> <li>[1] Disable = SNMP is disabled and no traps are sent.</li> </ul>
CLI: 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. <b>Note:</b> For this 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.
EMS: Keep Alive Trap Port [KeepAliveTrapPort]	Defines the port to which keep-alive traps are sent. The valid range is 0 - 65534. The default is port 162.
[SendKeepAliveTrap]	Enables keep-alive traps and sends them every 9/10 of the time as defined by the NATBindingDefaultTimeout parameter. <ul style="list-style-type: none"> <li>[0] = Disable</li> <li>[1] = Enable</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
CLI: sys-oid [SNMPSysOid]	Defines the base product system OID. The default is eSNMP_AC_PRODUCT_BASE_OID_D. <b>Note:</b> For this parameter to take effect, a device reset is required.
[SNMPTrapEnterpriseOid]	Defines the Trap Enterprise OID. The default is eSNMP_AC_ENTERPRISE_OID. The inner shift of the trap in the AcTrap subtree is added to the end of the OID in this parameter. <b>Note:</b> For this parameter to take effect, a device reset is required.
[acUserInputAlarmDescription]	Defines the description of the input alarm.

Parameter	Description
<b>[acUserInputAlarmSeverity]</b>	Defines the severity of the input alarm.
<b>[AlarmHistoryTableMaxSize]</b>	<p>Defines the maximum number of rows in the Alarm History table. This parameter can be controlled by the Config Global Entry Limit MIB (located in the Notification Log MIB). The valid range is 50 to 1000. The default is 500.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
CLI: engine-id <b>[SNMPEngineIDString]</b>	<p>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.</p> <p>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</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>Before setting this parameter, all SNMPv3 users must be deleted; otherwise, the parameter setting is ignored.</li> <li>If the supplied key does not pass validation of the 12 Hex values input or it is set with the default value, the engine ID is generated according to RFC 3411.</li> </ul>
<b>Web: SNMP Trap Destination Parameters</b> EMS: Network > SNMP Managers Table CLI: configure system/snmp trap destination <b>Note:</b> Up to five SNMP trap managers can be defined.	
SNMP Manager <b>[SNMPManagerIsUsed_x]</b>	<p>Determines the validity of the parameters (IP address and port number) of the corresponding SNMP Manager used to receive SNMP traps.</p> <ul style="list-style-type: none"> <li><b>[0]</b> (Check box cleared) = Disabled (default)</li> <li><b>[1]</b> (Check box selected) = Enabled</li> </ul>
Web: IP Address EMS: Address CLI: ip-address <b>[SNMPManagerTableIP_x]</b>	<p>Defines the IP address of the remote host used as an SNMP Manager. The device sends SNMP traps to this IP address. Enter the IP address in dotted-decimal notation, e.g., 108.10.1.255.</p>
Web: Trap Port EMS: Port CLI: port <b>[SNMPManagerTrapPort_x]</b>	<p>Defines the port number of the remote SNMP Manager. The device sends SNMP traps to this port.</p> <p>The valid SNMP trap port range is 100 to 4000. The default port is 162.</p>
Web: Trap Enable CLI: send-trap <b>[SNMPManagerTrapSendingEnabled_x]</b>	<p>Enables the sending of traps to the corresponding SNMP manager.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Sending is disabled.</li> <li><b>[1]</b> Enable = (Default) Sending is enabled.</li> </ul>
Web: Trap User CLI: trap-user <b>[SNMPManagerTrapUser_x]</b>	<p>Defines the SNMPv3 USM user or SNMPv2 user to associate with the trap destination. This determines the trap format, authentication level, and encryption level. By default, it is associated with the SNMPv2 user (SNMP trap community string). The valid value is a string.</p>
Web: Trap Manager Host Name	Defines an FQDN of the remote host used as an SNMP manager.

Parameter	Description
CLI: manager-host-name <b>[SNMPTrapManagerHostName]</b>	The resolved IP address replaces the last entry in the Trap Manager table (defined by the SNMPManagerTableIP parameter) and the last trap manager entry of snmpTargetAddrTable in the snmpTargetMIB. For example: 'mngtr.corp.mycompany.com'. The valid range is a string of up to 99 characters.
<b>SNMP Community String Parameters</b>	
Community String CLI: ro-community-string <b>[SNMPReadOnlyCommunityString_x]</b>	Defines up to five read-only SNMP community strings (up to 19 characters each). The default string is 'public'.
Community String CLI: rw-community-string <b>[SNMPReadWriteCommunityString_x]</b>	Defines up to five read/write SNMP community strings (up to 19 characters each). The default string is 'private'.
Trap Community String CLI: community-string <b>[SNMPTrapCommunityString]</b>	Defines the Community string used in traps (up to 19 characters). The default string is 'trapuser'.
<b>SNMP Trusted Managers Table</b>	
Web: SNMP Trusted Managers CLI: configure system > snmp > trusted-managers <b>[SNMPTrustedMgr_x]</b>	Defines up to five IP addresses of remote trusted SNMP managers from which the SNMP agent accepts and processes SNMP Get and Set requests. <b>Notes:</b> <ul style="list-style-type: none"> <li>By default, the SNMP agent accepts SNMP Get and Set requests from any IP address, as long as the correct community string is used in the request. Security can be enhanced by using Trusted Managers, which is an IP address from which the SNMP agent accepts and processes SNMP requests.</li> <li>If no values are assigned to these parameters any manager can access the device.</li> <li>Trusted managers can work with all community strings.</li> </ul>
<b>SNMP V3 Users Table</b>	
Web/EMS: SNMP V3 Users CLI: configure system > snmp v3-users <b>[SNMPUsers]</b>	This <i>parameter</i> table defines SNMP v3 users. The format of this parameter is as follows: <b>[SNMPUsers]</b> FORMAT SNMPUsers_Index = SNMPUsers_Username, SNMPUsers_AuthProtocol, SNMPUsers_PrivProtocol, SNMPUsers_AuthKey, SNMPUsers_PrivKey, SNMPUsers_Group; <b>[SNMPUsers]</b> 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. <b>Note:</b> For a description of this table, see 'Configuring SNMP V3 Users' on page 78.

## 59.2.5 CLI Parameters

The command-line interface (CLI) parameters are described in the table below.

**CLI Parameters**

Parameter	Description
CLI: aaa authentication login tacacs+ <b>[TacPlusEnable]</b>	Enables the Terminal Access Controller Access-Control System (TACACS+) remote authentication protocol and user authentication for CLI login. <ul style="list-style-type: none"> <li><b>[0]</b> = Disabled (default)</li> <li><b>[1]</b> = Enabled</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
CLI: tacacs-server host <host-ip> <b>[TacPlusServerIP]</b>	Defines the IP address (in dotted-decimal notation) of the TACACS+ primary authentication server.
CLI: tacacs-server host <host-ip> <b>[TacPlusSecondaryServerIP]</b>	Defines the IP address (in dotted-decimal notation) of the TACACS+ secondary authentication server.
CLI: tacacs-server port <port-num> <b>[TacPlusPort]</b>	Defines the TACACS+ authentication port (UDP) for authenticating with the RADIUS server. The valid value range is 1 to 15. The default is 49.
CLI: tacacs-server timeout <seconds> <b>[TacPlusTimeout]</b>	Defines the TACACS+ response timeout (in seconds). If no response is received within this period, retransmission is required. The valid value range is 1 to 15. The default is 5.
CLI: tacacs-server key <password> <b>[TacPlusSharedSecret]</b>	Defines the TACACS+ shared secret between client and server. The valid value can be a string of up to 64 characters. The default is "msbg".

## 59.2.6 TR-069 Parameters

The TR-069 parameters are described in the table below.

**TR-069 Parameters**

Parameter	Description
Web: TR069 CLI: service <b>[TR069ServiceEnable]</b>	Enables TR-069 management. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (Default)</li> <li><b>[1]</b> Enable</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: Connection Interface CLI: interface-type <b>[TR069WanEnable]</b>	Defines the device's network interface for the TR-069 connection. <ul style="list-style-type: none"> <li><b>[0]</b> LAN</li> <li><b>[1]</b> WAN (default)</li> </ul>



Parameter	Description
Web: Protocol CLI: protocol <b>[TR069Protocol]</b>	Defines the protocol used for the TR-069 connection. <ul style="list-style-type: none"> <li>▪ [0] HTTP (default)</li> <li>▪ [1] HTTPS</li> </ul>
Web: Port CLI: port <b>[TR069HTTPPort]</b>	Defines the local HTTP/S port used for TR-069. The valid range is 0 to 65535. The default is 82. <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: User Name CLI: acs-user-name <b>[TR069AcsUsername]</b>	Defines the login username that the device uses for authenticated access to the ACS. The valid value is a string of up to 256 characters. By default, no username is defined.
Web: Password CLI: acs-password <b>[TR069AcsPassword]</b>	Defines the login password that the device uses for authenticated access to the ACS. The valid value is a string of up to 256 characters. By default, no password is defined.
Web: URL CLI: connection-request-url <b>[TR069ConnectionRequestUrl]</b>	Defines the URL for the ACS connection request. For example, http://10.31.4.115:82/tr069/.
Web: User Name CLI: connection-request-user-name <b>[TR069ConnectionRequestUsername]</b>	Defines the connection request username used by the ACS to connect to the device. The valid value is a string of up to 256 characters. By default, no username is defined.
Web: Password CLI: connection-request-password <b>[TR069ConnectionRequestPassword]</b>	Defines the connection request password used by the ACS to connect to the device. The valid value is a string of up to 256 characters. By default, no password is defined.
Web: Inform Interval CLI: inform-interval <b>[TR069PeriodicInformInterval]</b>	Defines the inform interval (in seconds) at which the device periodically communicates with the ACS. Each time the device communicates with the ACS, the ACS sends a response indicating whether or not the ACS has an action to execute on the device. The valid value is 0 to 4294967295. The default is 60.
<b>[TR069RetryMinimumWaitInterval]</b>	Defines the minimum interval (in seconds) that the device waits before attempting again to communicate with the ACS after the previous communication attempt failure. The valid value is 1 to 65535. The default is 5.
CLI: debug-mode <b>[TR069DebugMode]</b>	Defines the debug mode level, which is the type of messages sent to the Syslog server. The valid value is between 0 and 3, where 0 (default) means no debug messages are sent and 3 is all message types are sent.



## 59.2.7 Serial Parameters

The RS-232 serial parameters are described in the table below.

**Serial Parameters**

Parameter	Description
[DisableRS232]	<p>Enables the device's RS-232 (serial) port.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Enabled</li> <li>▪ <b>[1]</b> = (Default) Disabled</li> </ul> <p>The RS-232 serial port can be used to change the networking parameters and view error/notification messages. For how to establish a serial communication with the device, refer to the <i>Installation Manual</i>.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: Baud Rate [SerialBaudRate]	<p>Defines the RS-232 baud rate.</p> <p>The valid values include the following: 1200, 2400, 9600, 14400, 19200, 38400, 57600, or 115200 (default).</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: Data [SerialData]	<p>Defines the RS-232 data bit.</p> <ul style="list-style-type: none"> <li>▪ <b>[7]</b> = 7-bit</li> <li>▪ <b>[8]</b> = (Default) 8-bit</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: Parity [SerialParity]	<p>Defines the RS-232 polarity.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) None</li> <li>▪ <b>[1]</b> = Odd</li> <li>▪ <b>[2]</b> = Even</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: Stop [SerialStop]	<p>Defines the RS-232 stop bit.</p> <ul style="list-style-type: none"> <li>▪ <b>[1]</b> = (Default) 1-bit (default)</li> <li>▪ <b>[2]</b> = 2-bit</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: Flow Control [SerialFlowControl]	<p>Defines the RS-232 flow control.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) None</li> <li>▪ <b>[1]</b> = Hardware</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>

## 59.3 Debugging and Diagnostics Parameters

This subsection describes the device's debugging and diagnostic parameters.

### 59.3.1 General Parameters

The general debugging and diagnostic parameters are described in the table below.

**General Debugging and Diagnostic Parameters**

Parameter	Description
CLI: enablesecsyslog <b>[EnableSecSyslog]</b>	<p>Enables the reporting of security-related events for the data-router networking. When enabled, the data-router access list rules, configured using the access-list CLI command, which are set to "log", send Syslog messages whenever traffic matching the access list is encountered.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Disabled</li> <li>▪ <b>[1]</b> = Enabled</li> </ul>
EMS: Enable Diagnostics <b>[EnableDiagnostics]</b>	<p>Determines the method for verifying correct functioning of the different hardware components on the device. On completion of the 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"> <li>▪ <b>[0]</b> = (Default) Rapid and Enhanced self-test mode.</li> <li>▪ <b>[1]</b> = Detailed self-test mode (full test of DSPs, PCM, Switch, LAN, PHY and Flash).</li> <li>▪ <b>[2]</b> = A quicker version of the Detailed self-test mode (full test of DSPs, PCM, Switch, LAN, PHY, but partial test of Flash).</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Enable LAN Watchdog <b>[EnableLanWatchDog]</b>	<p>Enables the LAN watchdog feature.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>When LAN watchdog is enabled, the device's overall communication integrity is checked periodically. If no communication is detected for about three minutes, the device performs a self test:</p> <ul style="list-style-type: none"> <li>▪ If the self-test succeeds, the problem is a logical link down (i.e., Ethernet cable disconnected on the switch side) and the Busy Out mechanism is activated if enabled (i.e., the parameter EnableBusyOut is set to 1).</li> <li>▪ If the self-test fails, the device restarts to overcome internal fatal communication error.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ Enable LAN watchdog is relevant only if the Ethernet connection is full duplex.</li> </ul>
<b>[LifeLineType]</b>	<p>Defines the condition(s) upon which the Lifeline analog (FXS) feature is activated. The Lifeline feature can be activated upon a power outage or network failure (i.e., loss of IP connectivity). Upon any of these conditions, the Lifeline feature provides PSTN connectivity and thus call continuity for the FXS phone users.</p> <p>If the device is in Lifeline mode and the scenario that caused it to enter Lifeline (e.g., power outage) no longer exists (e.g., power returns), the device exits Lifeline and operates as normal.</p>

Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Lifeline is activated upon power outage.</li> <li>▪ <b>[1]</b> = Lifeline is activated upon power outage.</li> <li>▪ <b>[2]</b> = Lifeline is activated upon a power outage, network failure (logical link disconnection), or when the Trunk Group is in Busy Out state (see the EnableBusyOut parameter).</li> </ul> <p>The Lifeline (FXS) phone is connected to FXS Port 1. FXS Port 1 connects to the POTS (Lifeline) phone as well as to the PSTN / PBX, using a splitter cable.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ This parameter is applicable only to FXS interfaces.</li> <li>▪ To enable Lifeline upon a network failure, the LAN watch dog must be activated (i.e., set the parameter EnableLANWatchDog to 1).</li> <li>▪ The number of supported Lifelines depends on the device's hardware configuration. For the combined FXS/FXO configuration, one Lifeline is available; for the 12-FXS configuration, up to three Lifelines are available.</li> <li>▪ For information on Lifeline cabling, refer to the Installation Manual.</li> </ul>
Web: Delay After Reset <b>[sec]</b> CLI: delay-after-reset <b>[GWAppDelayTime]</b>	<p>Defines the time interval (in seconds) that the device's operation is delayed after a reset.</p> <p>The valid range is 0 to 45. The default is 7 seconds.</p> <p><b>Note:</b> This feature helps overcome connection problems caused by some LAN routers or IP configuration parameters' modifications by a DHCP server.</p>
<b>[EnableAutoRAITransmitBER]</b>	<p>Enables the device to send a remote alarm indication (RAI) when the bit error rate (BER) is greater than 0.001.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Web: Ignore BRI LOS Alarm CLI: ignore-bri-los-alarm <b>[IgnoreBRILOSAAlarm]</b>	<p>Enables the device to ignore LOS alarms received from the BRI user-side trunk and attempts to make a call (relevant for IP-to-Tel calls).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable</li> <li>▪ <b>[1]</b> Enable (default)</li> </ul>

### 59.3.2 SIP Test Call Parameters

The SIP Signaling Test Call parameters are described in the table below.

**SIP Test Call Parameters**

Parameter	Description
Web: Test Call DTMF String CLI: testcall-dtmf-string <b>[TestCallDtmfString]</b>	<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". An empty string means that no DTMF is played.</p>
Web: Test Call ID CLI: testcall-id <b>[TestCallID]</b>	<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</p>

Parameter	Description
	<p>defined.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is only for testing incoming calls destined to this prefix number.</li> <li>This feature is applicable to all applications (GW/IP-to-IP and SBC).</li> </ul>
<p>Web: SBC Test ID</p> <p>CLI: sbc-test-id</p> <p><b>[SBCtestID]</b></p>	<p>Defines the SBC test call prefix (ID) for identifying SBC test calls that traverse the device to register with an external routing entity such as an IP PBX or proxy server.</p> <p>This parameter functions together with the TestCallID parameter, which defines the prefix of the simulated endpoint. Upon receiving an incoming call with this prefix, the device removes the prefix, enabling it to forward the test call to the external entity. Upon receiving the call from the external entity, the device identifies the call as a test call according to its prefix, defined by the TestCallID, and then sends the call to the simulated endpoint.</p> <p>For example, assume SBCTestID is set to 4 and TestCallID to 2. If a call is received with called destination 4200, the device removes the prefix 4 and routes the call to the IP PBX. When it receives the call from the IP PBX, it identifies the call as a test call (i.e., prefix 2) and therefore, sends it to the simulated endpoint.</p> <p>The valid value can be any string of up to 15 characters. By default, no number is defined.</p> <p><b>Note:</b> This feature is applicable only to the SBC application.</p>
<b>Test Call Table</b>	
<p>Web: Test Call Table</p> <p>CLI: configure system &gt; test-call &gt; test-call-table</p> <p><b>[Test_Call]</b></p>	<p>Defines the local and remote endpoints to be tested.</p> <p>[ Test_Call ]</p> <p>FORMAT Test_Call_Index = Test_Call_EndpointURI, Test_Call_CalledURI, Test_Call_RouteBy, Test_Call_IPGroupID, Test_Call_DestAddress, Test_Call_DestTransportType, Test_Call_SRD, Test_Call_ApplicationType, Test_Call_AutoRegister, Test_Call_UserName, Test_Call_Password, Test_Call_CallParty, Test_Call_MaxChannels, Test_Call_CallDuration, Test_Call_CallsPerSecond, Test_Call_TestMode, Test_Call_TestDuration, Test_Call_Play, Test_Call_ScheduleInterval;</p> <p>[Test_Call]</p> <p><b>Note:</b> For a description of this table, see 'Configuring Test Calls' on page 643.</p>

### 59.3.3 Syslog, CDR and Debug Parameters

The Syslog, CDR and debug parameters are described in the table below.

#### Syslog, CDR and Debug Parameters

Parameter	Description
<p>Web: Enable Syslog</p> <p>EMS: Syslog enable</p> <p>CLI: syslog</p> <p><b>[EnableSyslog]</b></p>	<p>Determines whether the device sends logs and error messages (e.g., CDRs) generated by the device to a Syslog server.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>

Parameter	Description
	<b>Notes:</b> <ul style="list-style-type: none"> <li>If you enable Syslog, you must enter an IP address of the Syslog server (using the SyslogServerIP parameter).</li> <li>Syslog messages may increase the network traffic.</li> <li>To configure Syslog SIP message logging levels, use the GwDebugLevel parameter.</li> <li>By default, logs are also sent to the RS-232 serial port. For how to establish serial communication with the device, refer to the Installation Manual.</li> </ul>
Web/EMS: Syslog Server IP Address CLI: syslog-ip <b>[SyslogServerIP]</b>	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.
Web: Syslog Server Port EMS: Syslog Server Port Number CLI: syslog-port <b>[SyslogServerPort]</b>	Defines the UDP port of the Syslog server.  The valid range is 0 to 65,535. The default port is 514.
CLI: mx-syslog-lgth <b>[MaxBundleSyslogLength]</b>	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.  <b>Note:</b> This parameter is applicable only if the GwDebugLevel parameter is set to 7.
Web: CDR Server IP Address EMS: IP Address of CDR Server CLI: cdr-srvr-ip-adrr <b>[CDRSyslogServerIP]</b>	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.  <b>Notes:</b> <ul style="list-style-type: none"> <li>The CDR messages are sent to UDP port 514 (default Syslog port).</li> <li>This mechanism is active only when Syslog is enabled (i.e., the parameter EnableSyslog is set to 1).</li> </ul>
Web/EMS: CDR Report Level CLI: cdr-report-level <b>[CDRReportLevel]</b>	Enables media- and signaling-related CDRs to be sent to a Syslog server and determines the call stage at which they are sent. <ul style="list-style-type: none"> <li><b>[0]</b> None = (Default) CDRs are not used.</li> <li><b>[1]</b> End Call = CDR is sent to the Syslog server at the end of each call.</li> <li><b>[2]</b> Start &amp; End Call = CDR report is sent to Syslog at the start and end of each call.</li> <li><b>[3]</b> Connect &amp; End Call = CDR report is sent to Syslog at connection and at the end of each call.</li> <li><b>[4]</b> Start &amp; End &amp; Connect Call = CDR report is sent to Syslog at the start, at connection, and at the end of each call.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>For the SBC application, this parameter enables only signaling-related CDRs. To enable media-related CDRs for SBC calls, use the MediaCDRReportLevel parameter.</li> <li>The CDR Syslog message complies with RFC 3161 and is</li> </ul>

Parameter	Description
	<p>identified by: Facility = 17 (local1) and Severity = 6 (Informational).</p> <ul style="list-style-type: none"> <li>This mechanism is active only when Syslog is enabled (i.e., the parameter EnableSyslog is set to 1).</li> </ul>
Web: Media CDR Report Level <b>[MediaCDRReportLevel]</b>	<p>Enables media-related CDRs of SBC calls to be sent to a Syslog server and determines the call stage at which they are sent.</p> <ul style="list-style-type: none"> <li><b>[0]</b> None = (Default) No media-related CDR is sent.</li> <li><b>[1]</b> End Media = Sends a CDR only at the end of the call.</li> <li><b>[2]</b> Start &amp; End Media = Sends a CDR once the media starts. In some calls it may only be after the call is established, but in other calls the media may start at ringback tone. A CDR is also sent upon termination (end) of the media in the call.</li> <li><b>[3]</b> Update &amp; End Media = Sends a CDR when an update occurs in the media of the call. For example, a call starts and a ringback tone occurs, a re-INVITE is sent for a fax call and as a result, a CDR with the MediaReportType field set to "Update" is sent, as the media was changed from voice to T.38. A CDR is also sent upon termination (end) of the media in the call.</li> <li><b>[4]</b> Start &amp; End &amp; Update Media = Sends a CDR at the start of the media, upon an update in the media (if occurs), and at the end of the media.</li> </ul> <p><b>Note:</b> To enable CDR generation as well as enable signaling-related CDRs, use the CDRReportLevel parameter.</p>
Web/EMS: Debug Level CLI: debug-level <b>[GwDebugLevel]</b>	<p>Defines the Syslog debug logging level.</p> <ul style="list-style-type: none"> <li><b>[0]</b> 0 = (Default) Debug is disabled.</li> <li><b>[1]</b> 1 = Flow debugging is enabled.</li> <li><b>[5]</b> 5 = Flow, device interface, stack interface, session manager, and device interface expanded debugging are enabled.</li> <li><b>[7]</b> 7 = This option is recommended when the device is running under "heavy" traffic. In this mode: <ul style="list-style-type: none"> <li>✓ The Syslog debug level automatically changes between level 5, level 1, and level 0, depending on the device's CPU consumption so that VoIP traffic isn't affected.</li> <li>✓ Syslog messages are bundled into a single UDP packet, after which they are sent to a Syslog server (bundling size is determined by the MaxBundleSyslogLength parameter). Bundling reduces the number of UDP Syslog packets, thereby improving CPU utilization.</li> </ul> </li> </ul> <p>Note that when this option is used, in order to read Syslog messages with Wireshark, a special plug-in (i.e., acsyslog.dll) must be used. Once the plug-in is installed, the Syslog messages are decoded as "AC SYSLOG" and are displayed using the 'acsyslog' filter instead of the regular 'syslog' filter.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is typically set to 5 if debug traces are required. However, in cases of heavy traffic, option 7 is recommended.</li> <li>Options 2, 3, 4, and 6 are not recommended.</li> </ul>
Web: Syslog Facility Number EMS: SyslogFacility <b>[SyslogFacility]</b>	<p>Defines the Facility level (0 through 7) of the device's Syslog messages, according to RFC 3164. This allows you to identify Syslog messages generated by the device. This is useful, for example, if you collect the device's and other equipments' Syslog messages, at one single server. The device's Syslog messages can easily be identified and distinguished from other Syslog messages by its Facility level.</p>

Parameter	Description
	<p>Therefore, in addition to filtering Syslog messages according to IP address, the messages can be filtered according to Facility level.</p> <ul style="list-style-type: none"> <li>▪ <b>[16]</b> = (Default) local use 0 (local0)</li> <li>▪ <b>[17]</b> = local use 1 (local1)</li> <li>▪ <b>[18]</b> = local use 2 (local2)</li> <li>▪ <b>[19]</b> = local use 3 (local3)</li> <li>▪ <b>[20]</b> = local use 4 (local4)</li> <li>▪ <b>[21]</b> = local use 5 (local5)</li> <li>▪ <b>[22]</b> = local use 6 (local6)</li> <li>▪ <b>[23]</b> = local use 7 (local7)</li> </ul>
<p>Web: Activity Types to Report via Activity Log Messages <b>[ActivityListToLog]</b></p>	<p>Defines the Activity Log mechanism of the device, which sends log messages to a Syslog server for reporting certain types of Web operations according to the below user-defined filters.</p> <ul style="list-style-type: none"> <li>▪ <b>[pvc]</b> Parameters Value Change = Changes made on-the-fly to parameters. Note that the <i>ini</i> file parameter, EnableParametersMonitoring can also be used to set this option, using values <b>[0]</b> (disable) or <b>[1]</b> (enable).</li> <li>▪ <b>[afi]</b> Auxiliary Files Loading = Loading of auxiliary files.</li> <li>▪ <b>[dr]</b> Device Reset = Reset of device via the 'Maintenance Actions page. <b>Note:</b> For this option to take effect, a device reset is required.</li> <li>▪ <b>[fb]</b> Flash Memory Burning = Burning of files or parameters to flash (in 'Maintenance Actions page).</li> <li>▪ <b>[swu]</b> Device Software Update = cmp file loading via the Software Upgrade Wizard.</li> <li>▪ <b>[ard]</b> Access to Restricted Domains = Access to restricted domains, which include the following Web pages: <ul style="list-style-type: none"> <li>✓ (1) ini parameters (AdminPage)</li> <li>✓ (2) General Security Settings</li> <li>✓ (3) Configuration File</li> <li>✓ (5) Software Upgrade Key Status</li> <li>✓ (7) Web &amp; Telnet Access List</li> <li>✓ (8) WEB User Accounts</li> </ul> </li> <li>▪ <b>[naa]</b> Non-Authorized Access = Attempt to access the Web interface with a false or empty user name or password.</li> <li>▪ <b>[spc]</b> Sensitive Parameters Value Change = Changes made to sensitive parameters: <ul style="list-style-type: none"> <li>✓ (1) IP Address</li> <li>✓ (2) Subnet Mask</li> <li>✓ (3) Default Gateway IP Address</li> <li>✓ (4) ActivityListToLog</li> </ul> </li> <li>▪ <b>[ll]</b> Login and Logout = Every login and logout attempt.</li> </ul> <p>For example: ActivityListToLog = 'pvc', 'afi', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc'</p> <p><b>Note:</b> For the <i>ini</i> file, values must be enclosed in single quotation marks.</p>
<p>CLI: oamp-default-network-src data/voip <b>[OAMPDefaultNetworkSource]</b></p>	<p>Defines the network interface from where the device sends Syslog messages to a Syslog server.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Data (default) = Syslog messages are sent from the WAN interface.</li> <li>▪ <b>[1]</b> VoIP = Syslog messages are sent from the VoIP LAN interface</li> </ul>



Parameter	Description
	for OAMP.
CLI: isdn-facility-trace <b>[FacilityTrace]</b>	<p>Enables ISDN traces of Facility Information Elements (IE) for ISDN call diagnostics. This allows you to trace all the parameters contained in the Facility IE and view them in the Syslog.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this feature to be functional, the GWDebugLevel parameter must be enabled (i.e., set to at least level 1).</p>
Web: Debug Recording Destination IP CLI: configure system > logging > dbg-rec-dest-ip <b>[DebugRecordingDestIP]</b>	Defines the IP address of the server for capturing debug recording.
Web: Debug Recording Destination Port CLI: configure system > logging > dbg-rec-dest-port <b>[DebugRecordingDestPort]</b>	Defines the UDP port of the server for capturing debug recording. The default is 925.
Debug Recording Status CLI: configure system > logging > dbg-rec-status <b>[DebugRecordingStatus]</b>	<p>Activates or de-activates debug recording.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Stop (default)</li> <li><b>[1]</b> Start</li> </ul>
<b>Logging Filters Table</b>	
Web: Logging Filters Table CLI: configure system > logging > logging-filters <b>[LoggingFilters]</b>	<p>This table parameter defines logging filtering rules for Syslog messages and debug recordings. The format of this parameter is as follows:</p> <p><b>[ LoggingFilters ]</b>            FORMAT LoggingFilters_Index = LoggingFilters_Type,            LoggingFilters_Value, LoggingFilters_Syslog,            LoggingFilters_CaptureType;  <b>[ \LoggingFilters ]</b></p> <p><b>Note:</b> For a detailed description of this table, see 'Filtering Syslog Messages and Debug Recordings' on page 631.</p>

### 59.3.4 Resource Allocation Indication Parameters

The Resource Allocation Indication (RAI) parameters are described in the table below.

**RAI Parameters**

Parameter	Description
<b>[EnableRAI]</b>	<p>Enables RAI alarm generation if the device's busy endpoints exceed a user-defined threshold.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disable RAI (Resource Available Indication) service.</li> <li><b>[1]</b> = RAI service enabled and an SNMP</li> </ul>



Parameter	Description
	'acBoardCallResourcesAlarm' Alarm Trap is sent.
<b>[RAIHighThreshold]</b>	<p>Defines the high threshold percentage of total calls that are active (busy endpoints). When the percentage of the device's busy endpoints exceeds this high threshold, the device sends the SNMP acBoardCallResourcesAlarm alarm trap with a 'major' alarm status.</p> <p>The range is 0 to 100. The default is 90.</p> <p><b>Note:</b> The percentage of busy endpoints is calculated by dividing the number of busy endpoints by the total number of "enabled" endpoints (trunks are physically connected and synchronized with no alarms and endpoints are defined in the Trunk Group Table).</p>
<b>[RAILowThreshold]</b>	<p>Defines the low threshold percentage of total calls that are active (busy endpoints).</p> <p>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.</p> <p>The range is 0 to 100%. The default is 90%.</p>
<b>[RAILoopTime]</b>	<p>Defines the time interval (in seconds) that the device periodically checks call resource availability.</p> <p>The valid range is 1 to 200. The default is 10.</p>

## 59.4 Security Parameters

This subsection describes the device's security parameters.

### 59.4.1 General Parameters

The general security parameters are described in the table below.

**General Security Parameters**

Parameter	Description
<b>Firewall Table</b>	
Web/EMS: Internal Firewall Parameters CLI: configure voip > access-list <b>[AccessList]</b>	<p>This table parameter defines the device's access list (firewall), which defines network traffic filtering rules.</p> <p>The format of this parameter is as follows:  <b>[AccessList]</b>            FORMAT AccessList_Index = AccessList_Source_IP, AccessList_Source_Port, AccessList_PrefixLen, AccessList_Source_Port, AccessList_Start_Port, AccessList_End_Port, AccessList_Protocol, AccessList_Use_Specific_Interface, AccessList_Interface_ID, AccessList_Packet_Size, AccessList_Byte_Rate, AccessList_Byte_Burst, AccessList_Allow_Type;  <b>[AccessList]</b></p> <p>For example:            AccessList 10 = mgmt.customer.com, , , 32, 0, 80, tcp, 1, OAMP, 0, 0, 0, allow;            AccessList 22 = 10.4.0.0, , , 16, 4000, 9000, any, 0, , 0, 0, 0, block;</p> <p>In the example above, Rule #10 allows traffic from the host 'mgmt.customer.com' destined to TCP ports 0 to 80 on interface OAMP</p>

Parameter	Description
	<p>(OAMP). Rule #22 blocks traffic from the subnet 10.4.xxx.yyy destined to ports 4000 to 9000.</p> <p><b>Note:</b> For a description of this table, see 'Configuring Firewall Settings' on page 131.</p>

## 59.4.2 HTTPS Parameters

The Secure Hypertext Transport Protocol (HTTPS) parameters are described in the table below.

**HTTPS Parameters**

Parameter	Description
Web: Secured Web Connection (HTTPS) EMS: HTTPS Only CLI: secured-connection <b>[HTTPSOnly]</b>	<p>Determines the protocol used to access the Web interface.</p> <ul style="list-style-type: none"> <li><b>[0]</b> HTTP and HTTPS (default).</li> <li><b>[1]</b> HTTPs Only = Unencrypted HTTP packets are blocked.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: HTTPS Port CLI: https-port <b>[HTTPSPort]</b>	<p>Defines the local Secured HTTPS port of the device. This parameter allows secure remote device Web management from the LAN. To enable secure Web management from the LAN, configure the desired port.</p> <p>The valid range is 1 to 65535 (other restrictions may apply within this range). The default port is 443.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web/EMS: HTTPS Cipher String CLI: https-cipher-string <b>[HTTPSCipherString]</b>	<p>Defines the Cipher string for HTTPS (in OpenSSL cipher list format). For the valid range values, refer to URL <a href="http://www.openssl.org/docs/apps/ciphers.html">http://www.openssl.org/docs/apps/ciphers.html</a>.</p> <p>The default is 'RC4:EXP' (Export encryption algorithms). For example, use 'ALL' for all ciphers suites (e.g., for ARIA encryption for TLS). The only ciphers available are RC4 and DES, and the cipher bit strength is limited to 56 bits.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>If the "Strong Encryption" Software License Key is enabled, the default of this parameter is changed to 'RC4:EXP', enabling RC-128bit encryption.</li> <li>The value 'ALL' can be configured only if the "Strong Encryption" Software License Key is enabled.</li> </ul>
Web: HTTP Authentication Mode EMS: Web Authentication Mode CLI: http-auth-mode <b>[WebAuthMode]</b>	<p>Determines the authentication mode used for the Web interface.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Basic Mode = (Default) Basic authentication (clear text) is used.</li> <li><b>[1]</b> Web Based Authentication = Digest authentication (MD5) is used.</li> </ul> <p><b>Note:</b> If you enable RADIUS login (i.e., the WebRADIUSLogin parameter is set to 1), you must set the WebAuthMode parameter to Basic Mode [0].</p>
Web: Requires Client Certificates for HTTPS connection CLI: req-client-cert <b>[HTTPSRequireClientCertificate]</b>	<p>Determines whether client certificates are required for HTTPS connection.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Client certificates are not required.</li> <li><b>[1]</b> Enable = Client certificates are required. The client certificate must be preloaded to the device and its matching private key must be installed on the managing PC. Time and date must be correctly set on</li> </ul>

Parameter	Description
	<p>the device for the client certificate to be verified.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a description on implementing client certificates, see 'Client Certificates' on page 98.</li> </ul>

### 59.4.3 SRTP Parameters

The Secure Real-Time Transport Protocol (SRTP) parameters are described in the table below.

**SRTP Parameters**

Parameter	Description
Web: Media Security EMS: Enable Media Security CLI: media-security-enable <b>[EnableMediaSecurity]</b>	<p>Enables Secure Real-Time Transport Protocol (SRTP).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) SRTP is disabled.</li> <li><b>[1]</b> Enable = SRTP is enabled.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web/EMS: Media Security Behavior <b>[MediaSecurityBehavior]</b>	<p>Determines the device's mode of operation when SRTP is used (i.e., when the parameter EnableMediaSecurity is set to 1).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Preferable = (Default) The device initiates encrypted calls. However, if negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted.</li> <li><b>[1]</b> Mandatory = The device initiates encrypted calls, but if negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected.</li> <li><b>[2]</b> Disable = The IP Profile for which this parameter is set does not support encrypted calls (i.e., SRTP).</li> <li><b>[3]</b> Preferable - Single Media = The device sends SDP with a single media ('m=') line only (e.g., m=audio 6000 RTP/AVP 4 0 70 96) with RTP/AVP and crypto keys. The remote UA can respond with SRTP or RTP parameters: <ul style="list-style-type: none"> <li>✓ If the remote SIP UA does not support SRTP, it uses RTP and ignores the crypto lines.</li> <li>✓ In the opposite direction, if the device receives an SDP offer with a single media (as shown above), it responds with SRTP (RTP/SAVP) if the EnableMediaSecurity parameter is set to 1. If SRTP is not supported (i.e., EnableMediaSecurity is set to 0), it responds with RTP.</li> </ul> </li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Before configuring this parameter, set the EnableMediaSecurity parameter to 1.</li> <li>If this parameter is set to Preferable <b>[3]</b> and two 'm=' lines are received in the SDP offer, the device prefers the SAVP (secure audio video profile) regardless of the order in the SDP.</li> <li>Option <b>[2]</b> Disable is applicable only to IP Profiles.</li> <li>This parameter can also be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 239).</li> </ul>

Parameter	Description
Web: Master Key Identifier (MKI) Size EMS: Packet MKI Size CLI: SRTP-tx-packet-MKI-size <b>[SRTPTxPacketMKISize]</b>	<p>Defines the size (in bytes) of the Master Key Identifier (MKI) in SRTP Tx packets.</p> <p>The range is 0 to 4. The default is 0 (i.e., new keys are generated without MKI).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For the GW/IP-to-IP application, the device only initiates the MKI size.</li> <li>You can also configure MKI size in an IP Profile.</li> <li>For the SBC application, the device can forward MKI size as is for SRTP-to-SRTP flows or override the MKI size during negotiation, using IP Profiles. This can be done on the inbound or outbound leg.</li> </ul>
Web: Symmetric MKI Negotiation EMS: Enable Symmetric MKI CLI: symmetric-mki <b>[EnableSymmetricMKI]</b>	<p>Enables symmetric MKI negotiation.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) The device includes the MKI in its 200 OK response according to the SRTPTxPacketMKISize parameter (if set to 0, then it is not included; if set to any other value, it is included with this value).</li> <li><b>[1]</b> Enable = The answer crypto line contains (or excludes) an MKI value according to the selected crypto line in the offer. For example, assume that the device receives an INVITE containing the following two crypto lines in SDP: <pre> a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:TAaxNnQt8/qLQMnDuG4vxYfWl6K7eBK/ufk04pR4 2^31 1:1 a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:bnuYZnMxSfUiGitviWJZmzr7OF3AiRO015Vnh0kH 2^31 </pre> <p>The first crypto line includes the MKI parameter "1:1". In the 200 OK response, the device selects one of the crypto lines (i.e., '2' or '3'). Typically, it selects the first line that supports the crypto suite. However, for SRTP-to-SRTP in SBC sessions, it can be determined by the remote side on the outgoing leg. If the device selects crypto line '2', it includes the MKI parameter in its answer SDP, for example:</p> <pre> a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:RlVyAlxV/qwBjkEklU4kSJyl3wCtYeZLq1/QFuxw 2^31 1:1 </pre> <p>If the device selects a crypto line that does not contain the MKI parameter, then the MKI parameter is not included in the crypto line in the SDP answer (even if the SRTPTxPacketMKISize parameter is set to any value other than 0).</p> </li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To enable symmetric MKI, the SRTPTxPacketMKISize parameter must be set to any value other than 0.</li> <li>You can also enable MKI negotiation per IP Profile.</li> </ul>
Web/EMS: SRTP offered Suites CLI: offer-srtp-cipher <b>[SRTPofferedSuites]</b>	<p>Defines the offered crypto suites (cipher encryption algorithms) for SRTP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) All available crypto suites.</li> <li><b>[1]</b> CIPHER SUITES AES CM 128 HMAC SHA1 80 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 80-bit tag.</li> <li><b>[2]</b> CIPHER SUITES AES CM 128 HMAC SHA1 32 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag.</li> <li><b>[4]</b> CIPHER SUITES ARIA CM 128 HMAC SHA1 80 = device uses ARIA encryption algorithm with a 128-bit key and HMAC-SHA1</li> </ul>

Parameter	Description
	<p>message authentication with a 32-bit tag.</p> <ul style="list-style-type: none"> <li>▪ <b>[8]</b> CIPHER SUITES ARIA CM 192 HMAC SHA1 80 = device uses ARIA encryption algorithm with a 192-bit key and HMAC-SHA1 message authentication with a 32-bit tag.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For enabling ARIA encryption, use the AriaProtocolSupport parameter.</li> <li>▪ This parameter also affects the selection of the crypto in the device's answer. For example, if the device receives an offer with two crypto lines containing HMAC_SHA1_80 and HMAC_SHA_32, it uses the HMAC_SHA_32 key in its SIP 200 OK response if the parameter is set to 2.</li> </ul>
Web: Aria Protocol Support CLI: ARIA-protocol-support <b>[AriaProtocolSupport]</b>	<p>Enables ARIA algorithm cipher encryption for SRTP. This is an alternative option to the existing support for the AES algorithm. ARIA is a symmetric key block cipher algorithm standard developed by the Korean National Security Research Institute.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To configure the ARIA bit-key encryption size (128 or 192 bit) with HMAC SHA-1 cryptographic hash function, use the SRTPOfferedSuites parameter.</li> <li>▪ For ARIA encryption of SRTP, the device must be installed with the relevant Software License Key.</li> </ul>
Web: Disable Authentication On Transmitted RTP Packets EMS: RTP AuthenticationDisable Tx CLI: RTP-authentication-disable-tx <b>[RTPAuthenticationDisableTx]</b>	<p>Enables authentication on transmitted RTP packets in a secured RTP session.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Enable (default)</li> <li>▪ <b>[1]</b> Disable</li> </ul>
Web: Disable Encryption On Transmitted RTP Packets EMS: RTP EncryptionDisable Tx CLI: RTP-encryption-disable-tx <b>[RTPEncryptionDisableTx]</b>	<p>Enables encryption on transmitted RTP packets in a secured RTP session.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Enable (default)</li> <li>▪ <b>[1]</b> Disable</li> </ul>
Web: Disable Encryption On Transmitted RTCP Packets EMS: RTCP EncryptionDisable Tx CLI: RTCP-encryption-disable-tx <b>[RTCPEncryptionDisableTx]</b>	<p>Enables encryption on transmitted RTCP packets in a secured RTP session.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Enable (default)</li> <li>▪ <b>[1]</b> Disable</li> </ul>

Parameter	Description
CLI: srtp-state-behavior-mode <b>[ResetSRTPStateUponRekey]</b>	<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"> <li><b>[0]</b> = (Default) Disabled. ROC is not reset on the device side.</li> <li><b>[1]</b> = Enabled. If the session expires causing a session refresh through a re-INVITE, the device or server generates a new key and the device resets the ROC index (and other SRTP fields) as done by the server, resulting in a synchronized SRTP.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This feature can also be configured for an IP Profile.</li> <li>If this feature is disabled and the server resets the ROC upon a re-key generation, one-way voice may occur.</li> </ul>

## 59.4.4 TLS Parameters

The Transport Layer Security (TLS) parameters are described in the table below.

### TLS Parameters

Parameter	Description
Web/EMS: TLS Version CLI: version <b>[TLSVersion]</b>	<p>Determines the supported versions of SSL/TLS (Secure Socket Layer/Transport Layer Security).</p> <ul style="list-style-type: none"> <li><b>[0]</b> SSL 2.0-3.0 and TLS 1.0 = (Default) SSL 2.0, SSL 3.0, and TLS 1.0 are supported.</li> <li><b>[1]</b> TLS 1.0 Only = only TLS 1.0 is used.</li> </ul> <p>When set to 0, SSL/TLS handshakes always start with SSL 2.0 and switch to TLS 1.0 if both peers support it. When set to 1, TLS 1.0 is the only version supported; clients attempting to contact the device using SSL 2.0 are rejected.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: TLS Client Re-Handshake Interval EMS: TLS Re Handshake Interval CLI: tls-re-hndshk-int <b>[TLSReHandshakeInterval]</b>	<p>Defines the time interval (in minutes) between TLS Re-Handshakes initiated by the device.</p> <p>The interval range is 0 to 1,500 minutes. The default is 0 (i.e., no TLS Re-Handshake).</p>
Web: TLS Mutual Authentication EMS: SIPS Require Client Certificate <b>[SIPSRequireClientCertificate]</b>	<p>Determines the device's behavior when acting as a server for TLS connections.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) The device does not request the client certificate.</li> <li><b>[1]</b> Enable = The device requires receipt and verification of the client certificate to establish the TLS connection.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>The SIPS certificate files can be changed using the parameters HTTPSCertFileName and HTTPSRootFileName.</li> </ul>

Parameter	Description
Web/EMS: Peer Host Name Verification Mode <b>[PeerHostNameVerificationMode]</b>	<p>Determines whether the device verifies the Subject Name of a remote certificate when establishing TLS connections.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default).</li> <li>▪ <b>[1]</b> Server Only = Verify Subject Name only when acting as a client for the TLS connection.</li> <li>▪ <b>[2]</b> Server &amp; Client = Verify Subject Name when acting as a server or client for the TLS connection.</li> </ul> <p>When a remote certificate is received and this parameter is not disabled, the value of SubjectAltName is compared with the list of available Proxies. If a match is found for any of the configured Proxies, the TLS connection is established.</p> <p>The comparison is performed if the SubjectAltName is either a DNS name (DNSName) or an IP address. If no match is found and the SubjectAltName is marked as 'critical', the TLS connection is not established. If DNSName is used, the certificate can also use wildcards ("*") to replace parts of the domain name.</p> <p>If the SubjectAltName is not marked as 'critical' and there is no match, the CN value of the SubjectName field is compared with the parameter TLSRemoteSubjectName. If a match is found, the connection is established. Otherwise, the connection is terminated.</p> <p><b>Note:</b> If you set this parameter to <b>[2]</b> (Server &amp; Client), for this functionality to operate, you also need to set the SIPSPRequireClientCertificate parameter to <b>[1]</b> (Enable).</p>
Web: TLS Client Verify Server Certificate EMS: Verify Server Certificate CLI: tls-vrfy-srvr-cert <b>[VerifyServerCertificate]</b>	<p>Determines whether the device, when acting as a client for TLS connections, verifies the Server certificate. The certificate is verified with the Root CA information.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> If Subject Name verification is necessary, the parameter PeerHostNameVerificationMode must be used as well.</p>
Web: Strict Certificate Extension Validation CLI: require-strict-cert <b>[RequireStrictCert]</b>	<p>Enables the validation of the extensions (keyUsage and extendedKeyUsage) of peer certificates. This validation ensures that the signing CA is authorized to sign certificates and that the end-entity certificate is authorized to negotiate a secure TLS connection.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Web/EMS: TLS Remote Subject Name CLI: tls-rmt-sub-name <b>[TLSRemoteSubjectName]</b>	<p>Defines the Subject Name that is compared with the name defined in the remote side certificate when establishing TLS connections.</p> <p>If the SubjectAltName of the received certificate is not equal to any of the defined Proxies Host names/IP addresses and is not marked as 'critical', the Common Name (CN) of the Subject field is compared with this value. If not equal, the TLS connection is not established. If the CN uses a domain name, the certificate can also use wildcards ("*") to replace parts of the domain name.</p> <p>The valid range is a string of up to 49 characters.</p> <p><b>Note:</b> This parameter is applicable only if the parameter PeerHostNameVerificationMode is set to 1 or 2.</p>



Parameter	Description
Web: Client Cipher String CLI: client-cipher-string <b>[TLSCClientCipherString]</b>	Defines the cipher-suite string for TLS clients. The valid value is up to 255 strings. The default is "ALL:!ADH". For example: TLSCClientCipherString = 'EXP' This parameter complements the HTTPSCipherString parameter (which affects TLS servers). For possible values and additional details, refer to: <a href="http://www.openssl.org/docs/apps/ciphers.html">http://www.openssl.org/docs/apps/ciphers.html</a>
CLI: pkey-size <b>[TLSPkeySize]</b>	Defines the key size (in bits) for RSA public-key encryption for newly self-signed generated keys for SSH. <ul style="list-style-type: none"> <li>▪ <b>[512]</b></li> <li>▪ <b>[768]</b></li> <li>▪ <b>[1024]</b> (default)</li> <li>▪ <b>[2048]</b></li> </ul>

## 59.4.5 SSH Parameters

Secure Shell (SSH) parameters are described in the table below.

### SSH Parameters

Parameter	Description
Web/EMS: Enable SSH Server CLI: ssh <b>[SSHServerEnable]</b>	Enables the device's embedded SSH server. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Web/EMS: Server Port cli: ssh-port <b>[SSHServerPort]</b>	Defines the port number for the embedded SSH server. Range is any valid port number. The default port is 22.
Web/EMS: SSH Admin Key CLI: ssh-admin-key <b>[SSHAdminKey]</b>	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.
Web: Require Public Key EMS: EMS: SSH Require Public Key CLI: ssh-require-public-key <b>[SSHRequirePublicKey]</b>	Enables RSA public keys for SSH. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) RSA public keys are optional if a value is configured for the parameter SSHAdminKey.</li> <li>▪ <b>[1]</b> = RSA public keys are mandatory.</li> </ul> <b>Note:</b> To define the key size, use the TLSPkeySize parameter.
Web: Max Payload Size EMS: SSH Max Payload Size CLI: ssh-max-payload-size <b>[SSHMaxPayloadSize]</b>	Defines the maximum uncompressed payload size (in bytes) for SSH packets. The valid value is 550 to 32768. The default is 32768.
Web: Max Binary Packet Size EMS: SSH Max Binary Packet Size CLI: ssh-max-binary-packet-size <b>[SSHMaxBinaryPacketSize]</b>	Defines the maximum packet size (in bytes) for SSH packets. The valid value is 582 to 35000. The default is 35000.
EMS: Telnet SSH Max Sessions CLI: ssh-max-sessions <b>[SSHMaxSessions]</b>	Defines the maximum number of simultaneous SSH sessions. The valid range is 1 to 2. The default is 2 sessions.
Web: Enable Last Login Message	Enables message display in SSH sessions of the time and



Parameter	Description
CLI: ssh-last-login-message <b>[SSHEnableLastLoginMessage]</b>	date of the last SSH login. The SSH login message displays the number of unsuccessful login attempts since the last successful login. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable</li> <li>▪ <b>[1]</b> Enable (default)</li> </ul> <b>Note:</b> The last SSH login information is cleared when the device is reset.
Web: Max Login Attempts CLI: ssh-max-login-attempts <b>[SSHMaxLoginAttempts]</b>	Defines the maximum SSH login attempts allowed for entering an incorrect password by an administrator before the SSH session is rejected.  The valid range is 1 to 3. the default is 3.

### 59.4.6 OCSP Parameters

The Online Certificate Status Protocol (OCSP) parameters are described in the table below.

**OCSP Parameters**

Parameter	Description
Web: Enable OCSP Server EMS: OCSP Enable CLI: enable <b>[OCSPEnable]</b>	Enables or disables certificate checking using OCSP. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Web: Primary Server IP EMS: OCSP Server IP CLI: server-ip <b>[OCSPServerIP]</b>	Defines the IP address of the OCSP server. The default IP address is 0.0.0.0.
Web: Secondary Server IP CLI: secondary-server-ip <b>[OCSPSecondaryServerIP]</b>	Defines the IP address (in dotted-decimal notation) of the secondary OCSP server (optional). The default IP address is 0.0.0.0.
Web: Server Port EMS: OCSP Server Port CLI: server-port <b>[OCSPServerPort]</b>	Defines the OCSP server's TCP port number. The default port number is 2560.
Web: Default Response When Server Unreachable EMS: OCSP Default Response CLI: default-response <b>[OCSPDefaultResponse]</b>	Determines the default OCSP behavior when the server cannot be contacted. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Reject = (Default) Rejects peer certificate.</li> <li>▪ <b>[1]</b> Allow = Allows peer certificate.</li> </ul>

## 59.4.7 IDS Parameters

The Intrusion Detection System (IDS) parameters are described in the table below.

**IDS Parameters**

Parameter	Description
Web: Intrusion Detection System (IDS) CLI: enable-ids <b>[EnableIDS]</b>	Enables the IDS feature. <ul style="list-style-type: none"> <li>[0] Disable (default)</li> <li>[1] Enable</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
CLI: ids-clear-period <b>[IDSArmClearPeriod]</b>	Defines the interval (in seconds) after which an IDS alarm is cleared from the Active Alarms table if no thresholds are crossed during this time. However, this "quiet" period must be at least twice the Threshold Window value. For example, if IDSArmClearPeriod is set to 20 sec and the Threshold Window is set to 15 sec, the IDSArmClearPeriod parameter is ignored and the alarm is cleared only after 30 seconds (2 x 15 sec). The valid value is 0 to 86400. The default is 300.
<b>IDS Policy Table</b>	
Web: IDS Policy Table <b>[IDSPolicy]</b>	Defines IDS Policies. The format of the ini file parameter is: [ IDSPolicy ] FORMAT IDSPolicy_Index = IDSPolicy_Name, IDSPolicy_Description; [ \IDSPolicy ] For a detailed description of this table, see 'Configuring IDS Policies' on page 137.
<b>IDS Rule Table</b>	
Web: IDS Rule Table <b>[IDSRule]</b>	Defines rules for the IDS Policies. The format of the ini file parameter is: [ IDSRule ] FORMAT IDSRule_Index = IDSRule_Policy, IDSRule_RuleID, IDSRule_Reason, IDSRule_ThresholdScope, IDSRule_ThresholdWindow, IDSRule_MinorAlarmThreshold, IDSRule_MajorAlarmThreshold, IDSRule_CriticalAlarmThreshold; [ \IDSRule ] For a detailed description of this table, see 'Configuring IDS Policies' on page 137.
<b>IDS Match Table</b>	
Web: IDS Match Table <b>[IDSMatch]</b>	Defines target rules per IDS Policy. The format of the ini file parameter is: [ IDSMatch ] FORMAT IDSMatch_Index = IDSMatch_SIPInterface, IDSMatch_ProxySet, IDSMatch_Subnet, IDSMatch_Policy; [ \IDSMatch ] For a detailed description of this table, see 'Assigning IDS Policies' on page 140.

## 59.5 RADIUS Parameters

The RADIUS parameters are described in the table below. For supported RADIUS attributes, see 'RADIUS Accounting CDR Attributes' on page 619.

### RADIUS Parameters

Parameter	Description
<b>RADIUS Accounting Parameters</b>	
Web: Enable RADIUS Access Control CLI: enable <b>[EnableRADIUS]</b>	Enables the RADIUS application. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (Default)</li> <li><b>[1]</b> Enable</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: Accounting Server IP Address CLI: accounting-server-ip <b>[RADIUSAccServerIP]</b>	Defines the IP address of the RADIUS accounting server.
Web: Accounting Port CLI: accounting-port <b>[RADIUSAccPort]</b>	Defines the port of the RADIUS accounting server. The default is 1646.
Web/EMS: RADIUS Accounting Type CLI: radius-accounting <b>[RADIUSAccountingType]</b>	Determines when the RADIUS accounting messages are sent to the RADIUS accounting server. <ul style="list-style-type: none"> <li><b>[0]</b> At Call Release = (Default) Sent at call release only.</li> <li><b>[1]</b> At Connect &amp; Release = Sent at call connect and release.</li> <li><b>[2]</b> At Setup &amp; Release = Sent at call setup and release.</li> </ul>
Web: AAA Indications EMS: Indications CLI: aaa-indications <b>[AAAIndications]</b>	Determines the Authentication, Authorization and Accounting (AAA) indications. <ul style="list-style-type: none"> <li><b>[0]</b> None = (Default) No indications.</li> <li><b>[3]</b> Accounting Only = Only accounting indications are used.</li> </ul>
<b>General RADIUS Parameters</b>	
Web: Use RADIUS for Web/Telnet Login EMS: Web Use Radius Login CLI: enable-mgmt-login <b>[WebRADIUSLogin]</b>	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"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>For RADIUS login authentication to function, you also need to set the following parameters: <ul style="list-style-type: none"> <li>✓ EnableRADIUS = 1 (Enable)</li> <li>✓ WebAuthMode = 0 (Basic Mode)</li> </ul> </li> <li>RADIUS authentication requires HTTP basic authentication, where the username and password are transmitted in clear text over the network. Therefore, it's recommended to set the HTTPSONly parameter to 1 in order to force the use of HTTPS, since the transport is encrypted.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>If using RADIUS authentication to log into the CLI, only the primary Web User Account, which has Security Administration access level, can access the device's CLI (see 'Configuring Web User Accounts' on page 58).</li> </ul>
Web: RADIUS Authentication Server IP Address EMS: RADIUS Auth Server IP CLI: auth-server-ip <b>[RADIUSAuthServerIP]</b>	Defines the IP address of the RADIUS authentication server. <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: RADIUS Authentication Server Port EMS: RADIUS Auth Server Port CLI: auth-server-port <b>[RADIUSAuthPort]</b>	Defines the port of the RADIUS Authentication Server. <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: RADIUS Shared Secret EMS: RADIUS Auth Server Secret CLI: shared-secret <b>[SharedSecret]</b>	Defines the 'Secret' used to authenticate the device to the RADIUS server. This should be a cryptically strong password.
<b>RADIUS Authentication Parameters</b>	
Web: Default Access Level CLI: default-access-level <b>[DefaultAccessLevel]</b>	Defines the default access level for the device when the RADIUS (authentication) response doesn't include an access level attribute. The valid range is 0 to 255. The default is 200 (i.e., Security Administrator).
Web: Device Behavior Upon RADIUS Timeout CLI: timeout-behavior <b>[BehaviorUponRadiusTimeout]</b>	Defines the device's response upon a RADIUS timeout. <ul style="list-style-type: none"> <li><b>[0]</b> Deny Access = Denies access.</li> <li><b>[1]</b> Verify Access Locally = (Default) Checks password locally.</li> </ul>
Web: Local RADIUS Password Cache Mode CLI: local-cache-mode <b>[RadiusLocalCacheMode]</b>	Determines the device's mode of operation regarding the timer (configured by the parameter RadiusLocalCacheTimeout) that determines the validity of the user name and password (verified by the RADIUS server). <ul style="list-style-type: none"> <li><b>[0]</b> Absolute Expiry Timer = When you access a Web page, the timeout doesn't reset, instead it continues decreasing.</li> <li><b>[1]</b> Reset Timer Upon Access = (Default) Upon each access to a Web page, the timeout always resets (reverts to the initial value configured by RadiusLocalCacheTimeout).</li> </ul>
Web: Local RADIUS Password Cache Timeout CLI: local-cache-timeout <b>[RadiusLocalCacheTimeout]</b>	Defines the time (in seconds) the locally stored user name and password (verified by the RADIUS server) are valid. When this time expires, the user name and password become invalid and a must be re-verified with the RADIUS server. The valid range is 1 to 0xFFFFFFFF. The default is 300 (5 minutes). <ul style="list-style-type: none"> <li><b>[-1]</b> = Never expires.</li> <li><b>[0]</b> = Each request requires RADIUS authentication.</li> </ul>
Web: RADIUS VSA Vendor ID CLI: vsa-vendor-id <b>[RadiusVSAVendorID]</b>	Defines the vendor ID that the device accepts when parsing a RADIUS response packet. The valid range is 0 to 0xFFFFFFFF. The default is 5003.

Parameter	Description
Web: RADIUS VSA Access Level Attribute CLI: vsa-access-level <b>[RadiusVSAAccessAttribute]</b>	Defines the code that indicates the access level attribute in the Vendor Specific Attributes (VSA) section of the received RADIUS packet. The valid range is 0 to 255. The default is 35.
<b>[MaxRADIUSSessions]</b>	Defines the number of concurrent calls that can communicate with the RADIUS server (optional). The valid range is 0 to 240. The default is 240.
EMS: RADIUS Auth Number of Retries <b>[RADIUSRetransmission]</b>	Defines the number of retransmission retries. The valid range is 1 to 10. The default is 3.
<b>[RadiusTO]</b>	Defines the time interval (measured in seconds) that the device waits for a response before a RADIUS retransmission is issued. The valid range is 1 to 30. The default is 10.

## 59.6 SIP Media Realm Parameters

The Media Realm parameters are described in the table below.

**Media Realm Parameters**

Parameter	Description
<b>Media Realm Table</b>	
Web: Media Realm Table EMS: VoIP > Media > Media Realm CLI: configure voip > media realm <b>[CpMediaRealm]</b>	<p>This table parameter defines the Media Realm table. The Media Realm table allows you to divide a Media-type interface (defined in the Multiple Interface table) into several realms, where each realm is specified by a UDP port range.</p> <p>The format of this parameter is as follows:</p> <p><b>[CpMediaRealm]</b>            FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd, CpMediaRealm_TransRateRatio, CpMediaRealm_IsDefault;  <b>[CpMediaRealm]</b></p> <p>For example,            CpMediaRealm 1 = Mrealm1, Voice, , 6600, 20, 6790, , 1;            CpMediaRealm 2 = Mrealm2, Voice, , 6800, 10, 6890; , 0;</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a detailed description of this table, see 'Configuring Media Realms' on page 168.</li> </ul>
<b>Bandwidth Management per Media Realm Table</b>	
Web: Bandwidth Management <b>[BWManagement]</b>	<p>This table parameter defines bandwidth management rules per Media Realm.</p> <p>The format of this parameter is as follows:</p> <p><b>[ BWManagement ]</b></p>

Parameter	Description
	<p>FORMAT BWManagement_Index = BWManagement_MediaRealmIndex, BWManagement_ThresholdIndex, BWManagement_RuleAction, BWManagement_Threshold, BWManagement_Hysteresis;</p> <p>[ \BWManagement ]</p> <p>Where ThresholdIndex is the bandwidth threshold rule type:</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> High Threshold Rule</li> <li>▪ <b>[1]</b> Critical Threshold Rule</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ This table can include up to two row entries (where 0 is the first index).</li> <li>▪ For a detailed description of this table, see 'Configuring Bandwidth Management per Media Realm' on page 173.</li> </ul>
Quality of Experience Parameters	
Web: Server IP CLI: server-ip <b>[QOEServerIP]</b>	<p>Defines the IP address of AudioCodes Session Experience Manager (SEM) server to where the quality experience reports are sent.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Port <b>[QOEPort]</b>	<p>Defines the port of the SEM server.</p> <p>The valid value range is 0 to 65534. The default is 5000.</p>
Web: Interface Name <b>[QOEInterfaceName]</b>	<p>Defines the IP network interface on which the quality experience reports are sent.</p> <p>The default is the OAMP interface.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Connection Mode CLI: connection-mode <b>[QOEConnectionMode]</b>	<p>Defines the connection between the device and the SEM.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Server = The device receives connection from the server.</li> <li>▪ <b>[1]</b> Client (default) = The device connects to the SEM.</li> <li>▪ <b>[2]</b> None</li> </ul> <p><b>Note:</b> Currently, only the client connection is supported.</p>
Web: Information Level CLI: information-level <b>[QOEInformationLevel]</b>	<p>Defines the level (i.e., amount of detail) of voice quality information that is sent to the SEM server.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Standard (default)</li> <li>▪ <b>[1]</b> Enhanced</li> <li>▪ <b>[2]</b> Debug</li> </ul>
Web: Use Mos LQ CLI: use-mos-lq <b>[QOEUseMosLQ]</b>	<p>Enables the reporting of the MOS-LQ (listening quality). If disabled, the MOS-CQ (conversational quality) is reported. MOS-LQ measures the quality of audio for listening purposes only. MOS-LQ does not take into account bi-directional effects such as delay and echo. MOS-CQ takes into account listening quality in both directions, as well as the bi-directional effects.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Media Realm > Quality of Experience Table	

Parameter	Description
Web: Media Realm > Quality Of Experience EMS: Media > Media Realm > Voice Quality Rules <b>[QOERules]</b>	This table configures Quality of Experience parameters per Media Realm. <b>[ QOERules ]</b> ORMAT QOERules_Index = QOERules_MediaRealmIndex, QOERules_RuleIndex, QOERules_MonitoredParam, QOERules_Direction, QOERules_Profile, QOERules_GreenYellowThreshold, QOERules_GreenYellowHysteresis, QOERules_YellowRedThreshold, QOERules_YellowRedHysteresis, QOERules_GreenYellowOperation, QOERules_GreenYellowOperationDetails, QOERules_YellowRedOperation, QOERules_YellowRedOperationDetails; <b>[ \QOERules ]</b> <b>Note:</b> For a detailed description of this table, see Configuring Quality of Experience Parameters per Media Realm on page 170.

## 59.7 Control Network Parameters

### 59.7.1 IP Group, Proxy, Registration and Authentication Parameters

The proxy server, registration and authentication SIP parameters are described in the table below.

**Proxy, Registration and Authentication SIP Parameters**

Parameter	Description
<b>IP Group Table</b>	
Web: IP Group Table EMS: Endpoints > IP Group CLI: configure voip > control-network ip-group <b>[IPGroup]</b>	This table configures IP Groups. The ini file format of this parameter is as follows: <b>[IPGroup]</b> FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description, IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_EnableSurvivability, IPGroup_ServingIPGroup, IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable, IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm, IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList, IPGroup_EnableSBCCClientForking, IPGroup_SourceUriInput, IPGroup_DestUriInput, IPGroup_ContactName; <b>[/IPGroup]</b> <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a description of this table, see 'Configuring IP Groups' on page 204.</li> </ul>
Authentication per Port Table	



Parameter	Description
Web: Authentication Table EMS: SIP Endpoints > Authentication CLI: configure voip/gw analoggw authentication <b>[Authentication]</b>	<p>This table parameter defines a user name and password for authenticating each device port. The format of this parameter is as follows:</p> <p><b>[Authentication]</b>  FORMAT Authentication_Index = Authentication_UserId, Authentication_UserPassword, Authentication_Module, Authentication_Port;  <b>[Authentication]</b></p> <p>Where,</p> <ul style="list-style-type: none"> <li>Module = Module number, where 1 denotes the module in Slot 1</li> <li>Port = Port number, where 1 denotes the Port 1 of the module</li> </ul> <p>For example:  Authentication 1 = lee,1552,1,2; (user name "lee" with password 1552 for authenticating Port 2 of Module 1)</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The indexing of this parameter starts at 0.</li> <li>For a description of this table, see Configuring Authentication on page 395.</li> </ul>
<b>Account Table</b>	
Web: Account Table EMS: SIP Endpoints > Account CLI: configure voip > sip-definition account <b>[Account]</b>	<p>This table parameter configures the Account table for registering and/or authenticating (digest) Trunk Groups or IP Groups (e.g., an IP-PBX) to another Serving IP Group (e.g., an Internet Telephony Service Provider - ITSP). The format of this parameter is as follows:</p> <p><b>[Account]</b>  FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup, Account_ServingIPGroup, Account_Username, Account_Password, Account_HostName, Account_Register, Account_ContactUser, Account_ApplicationType;  <b>[Account]</b></p> <p>For example:  Account 1 = 1, -1, 1, user, 1234, acl, 1, ITSP1, 0;</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring Account Table' on page 219.</p>
<b>Proxy Registration Parameters</b>	
Web: Use Default Proxy EMS: Proxy Used CLI: enable-proxy <b>[IsProxyUsed]</b>	<p>Enables the use of a SIP proxy server.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) Proxy isn't used and instead, the internal routing table is used.</li> <li><b>[1]</b> Yes = Proxy server is used. Define the IP address of the proxy server in the Proxy Sets table (see 'Configuring Proxy Sets Table' on page 213).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If you are not using a proxy server, you must define outbound IP call routing rules in the Outbound IP Routing Table (described in Configuring Outbound IP Routing Table on page 321).</li> <li>This parameter is applicable only to the GW/IP-to-IP application.</li> </ul>
Web/EMS: Proxy Name CLI: proxy-name <b>[ProxyName]</b>	<p>Defines the Home Proxy domain name. If specified, this name is used as the Request-URI in REGISTER, INVITE and other SIP messages, and as the host part of the To header in INVITE messages. If not specified, the Proxy IP address is used instead.</p>



Parameter	Description
	<p>The valid value is a string of up to 49 characters.</p> <p><b>Note:</b> This parameter functions together with the UseProxyIPasHost parameter.</p>
Web: Use Proxy IP as Host CLI: use-proxy-ip-as-host <b>[UseProxyIPasHost]</b>	<p>Enables the use of the proxy server's IP address (in dotted-decimal notation) as the host name in SIP From and To headers in REGISTER requests.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>If this parameter is disabled and the device registers to an IP Group (i.e., proxy server), it uses the string configured by the ProxyName parameter as the host name in the REGISTER's Request-URI and uses the string configured by the IP Group table parameter, SIPGroupName as the host name in the To and From headers. If the IP Group is configured with a Proxy Set that has multiple IP addresses, all the REGISTER messages sent to these proxies are sent with the same host name.</p> <p><b>Note:</b> If this parameter is disabled and the ProxyName parameter is not configured, the proxy's IP address is used as the host name in the REGISTER Request-URI.</p>
Web: Redundancy Mode EMS: Proxy Redundancy Mode CLI: redundancy-mode <b>[ProxyRedundancyMode]</b>	<p>Determines whether the device switches back to the primary Proxy after using a redundant Proxy.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Parking = (Default) The device continues working with a redundant (now active) Proxy until the next failure, after which it works with the next redundant Proxy.</li> <li><b>[1]</b> Homing = The device always tries to work with the primary Proxy server (i.e., switches back to the primary Proxy whenever it's available).</li> </ul> <p><b>Note:</b> To use this Proxy Redundancy mechanism, you need to enable the keep-alive with Proxy option, by setting the parameter EnableProxyKeepAlive to 1 or 2.</p>
Web: Proxy IP List Refresh Time EMS: IP List Refresh Time CLI: proxy-ip-lst-rfrsh-time <b>[ProxyIPListRefreshTime]</b>	<p>Defines the time interval (in seconds) between each Proxy IP list refresh.</p> <p>The range is 5 to 2,000,000. The default interval is 60.</p>
Web: Enable Fallback to Routing Table EMS: Fallback Used CLI: fallback-to-routing <b>[IsFallbackUsed]</b>	<p>Determines whether the device falls back to the Outbound IP Routing Table for call routing when Proxy servers are unavailable.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Fallback is not used.</li> <li><b>[1]</b> Enable = The Outbound IP Routing Table is used when Proxy servers are unavailable.</li> </ul> <p>When the device falls back to the Outbound IP Routing Table, it continues scanning for a Proxy. When the device locates an active Proxy, it switches from internal routing back to Proxy routing.</p> <p><b>Note:</b> To enable the redundant Proxies mechanism, set the parameter EnableProxyKeepAlive to 1 or 2.</p>
Web/EMS: Prefer Routing Table CLI: prefer-routing-table	<p>Determines whether the device's internal routing table takes precedence over a Proxy for routing calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) Only a Proxy server is used to route calls.</li> </ul>

Parameter	Description
<b>[PreferRouteTable]</b>	<ul style="list-style-type: none"> <li><b>[1]</b> Yes = The device checks the routing rules in the Outbound IP Routing Table for a match with the Tel-to-IP call. Only if a match is not found is a Proxy used.</li> </ul>
Web/EMS: Always Use Proxy CLI: always-use-proxy <b>[AlwaysSendToProxy]</b>	<p>Determines whether the device sends SIP messages and responses through a Proxy server.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Use standard SIP routing rules.</li> <li><b>[1]</b> Enable = All SIP messages and responses are sent to the Proxy server.</li> </ul> <p><b>Note:</b> This parameter is applicable only if a Proxy server is used (i.e., the parameter IsProxyUsed is set to 1).</p>
Web: SIP ReRouting Mode EMS: SIP Re-Routing Mode CLI: sip-rerouting-mode <b>[SIPReroutingMode]</b>	<p>Determines the routing mode after a call redirection (i.e., a 3xx SIP response is received) or transfer (i.e., a SIP REFER request is received).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Standard = (Default) INVITE messages that are generated as a result of Transfer or Redirect are sent directly to the URI, according to the Refer-To header in the REFER message, or Contact header in the 3xx response.</li> <li><b>[1]</b> Proxy = Sends a new INVITE to the Proxy. Note: This option is applicable only if a Proxy server is used and the parameter AlwaysSendtoProxy is set to 0.</li> <li><b>[2]</b> Routing Table = Uses the Routing table to locate the destination and then sends a new INVITE to this destination.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Gateway / IP-to-IP application.</li> <li>When this parameter is set to <b>[1]</b> and the INVITE sent to the Proxy fails, the device re-routes the call according to the Standard mode <b>[0]</b>.</li> <li>When this parameter is set to <b>[2]</b> and the INVITE fails, the device re-routes the call according to the Standard mode <b>[0]</b>. If DNS resolution fails, the device attempts to route the call to the Proxy. If routing to the Proxy also fails, the Redirect/Transfer request is rejected.</li> <li>When this parameter is set to <b>[2]</b>, the XferPrefix parameter can be used to define different routing rules for redirect calls.</li> <li>This parameter is disregarded if the parameter AlwaysSendToProxy is set to 1.</li> </ul>
Web/EMS: DNS Query Type CLI: dns-query <b>[DNSQueryType]</b>	<p>Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to resolve Proxy and Registrar servers and to resolve all domain names that appear in the SIP Contact and Record-Route headers.</p> <ul style="list-style-type: none"> <li><b>[0]</b> A-Record (default)</li> <li><b>[1]</b> SRV</li> <li><b>[2]</b> NAPTR</li> </ul> <p>If set to A-Record <b>[0]</b>, no NAPTR or SRV queries are performed.</p> <p>If set to SRV <b>[1]</b> and the Proxy/Registrar IP address parameter, Contact/Record-Route headers, or IP address defined in the Routing tables contain a domain name, an SRV query is performed. The device uses the first host name received from the SRV query. The device then performs a DNS A-record query for the host name to locate an IP address.</p> <p>If set to NAPTR <b>[2]</b>, an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR</p>

Parameter	Description
	<p>response. If the NAPTR query fails, an SRV query is performed according to the configured transport type.</p> <p>If the Proxy/Registrar IP address parameter, the domain name in the Contact/Record-Route headers, or the IP address defined in the Routing tables contain a domain name with port definition, the device performs a regular DNS A-record query.</p> <p>If a specific Transport Type is defined, a NAPTR query is not performed.</p> <p><b>Note:</b> To enable NAPTR/SRV queries for Proxy servers only, use the parameter ProxyDNSQueryType.</p>
Web: Proxy DNS Query Type CLI: proxy-dns-query <b>[ProxyDNSQueryType]</b>	<p>Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to discover Proxy servers.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> A-Record (default)</li> <li>▪ <b>[1]</b> SRV</li> <li>▪ <b>[2]</b> NAPTR</li> </ul> <p>If set to A-Record <b>[0]</b>, no NAPTR or SRV queries are performed.</p> <p>If set to SRV <b>[1]</b> and the Proxy IP address parameter contains a domain name without port definition (e.g., ProxyIP = domain.com), an SRV query is performed. The SRV query returns up to four Proxy host names and their weights. The device then performs DNS A-record queries for each Proxy host name (according to the received weights) to locate up to four Proxy IP addresses. Therefore, if the first SRV query returns two domain names and the A-record queries return two IP addresses each, no additional searches are performed.</p> <p>If set to NAPTR <b>[2]</b>, an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is performed according to the configured transport type.</p> <p>If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = domain.com:5080), the device performs a regular DNS A-record query.</p> <p>If a specific Transport Type is defined, a NAPTR query is not performed.</p> <p><b>Note:</b> When enabled, NAPTR/SRV queries are used to discover Proxy servers even if the parameter DNSQueryType is disabled.</p>
Web/EMS: Use Gateway Name for OPTIONS CLI: use-gw-name-for-opt <b>[UseGatewayNameForOptions]</b>	<p>Determines whether the device uses its IP address or gateway name in keep-alive SIP OPTIONS messages.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No = (Default) Use the device's IP address in keep-alive OPTIONS messages.</li> <li>▪ <b>[1]</b> Yes = Use 'Gateway Name' (SIPGatewayName) in keep-alive OPTIONS messages.</li> </ul> <p>The OPTIONS Request-URI host part contains either the device's IP address or a string defined by the parameter SIPGatewayName. The device uses the OPTIONS request as a keep-alive message to its primary and redundant Proxies (i.e., the parameter EnableProxyKeepAlive is set to 1).</p> <p><b>Note:</b> This parameter is applicable only to the Gateway / IP-to-IP application.</p>
Web/EMS: User Name CLI: user-name-4-auth <b>[UserName]</b>	<p>Defines the user name used for registration and Basic/Digest authentication with a Proxy/Registrar server.</p>

Parameter	Description
	<p>The default value is an empty string.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Gateway / IP-to-IP application.</li> <li>This parameter is applicable only if single device registration is used (i.e., the parameter AuthenticationMode is set to authentication per gateway).</li> <li>Instead of configuring this parameter, the Authentication table can be used (see Authentication on page 395).</li> </ul>
Web/EMS: Password CLI: password-4-auth <b>[Password]</b>	<p>Defines the password for Basic/Digest authentication with a Proxy/Registrar server. A single password is used for all device ports. The default is 'Default_Passwd'.</p> <p><b>Note:</b> Instead of configuring this parameter, the Authentication table can be used (see Authentication on page 395).</p>
Web/EMS: Cnonce CLI: cnonce-4-auth <b>[Cnonce]</b>	<p>Defines the Cnonce string used by the SIP server and client to provide mutual authentication.</p> <p>The value is free format, i.e., 'Cnonce = 0a4f113b'. The default is 'Default_Cnonce'.</p>
Web/EMS: Mutual Authentication Mode CLI: mutual-authentication <b>[MutualAuthenticationMode]</b>	<p>Determines the device's mode of operation when Authentication and Key Agreement (AKA) Digest Authentication is used.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Optional = (Default) Incoming requests that don't include AKA authentication information are accepted.</li> <li><b>[1]</b> Mandatory = Incoming requests that don't include AKA authentication information are rejected.</li> </ul>
Web/EMS: Challenge Caching Mode CLI: challenge-caching <b>[SIPChallengeCachingMode]</b>	<p>Determines the mode for Challenge Caching, which reduces the number of SIP messages transmitted through the network. The first request to the Proxy is sent without authorization. The Proxy sends a 401/407 response with a challenge. This response is saved for further uses. A new request is re-sent 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.</p> <ul style="list-style-type: none"> <li><b>[0]</b> 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.</li> <li><b>[1]</b> INVITE Only = Challenges issued for INVITE requests are cached. This prevents a mixture of REGISTER and INVITE authorizations.</li> <li><b>[2]</b> Full = Caches all challenges from the proxies.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Gateway IP-to-IP application.</li> <li>Challenge Caching is used with all proxies and not only with the active one.</li> </ul>
<b>Proxy IP Table</b>	
Web: Proxy IP Table EMS: Proxy IP CLI: configure voip > control-network proxy-ip	<p>This table parameter configures the Proxy Set table with Proxy Set IDs, each with up to five Proxy server IP addresses (or fully qualified domain name/FQDN). Each Proxy Set can be defined with a transport type (UDP, TCP, or TLS). The format of this parameter is as follows:</p>

Parameter	Description
<b>[ProxyIP]</b>	<p><b>[ProxyIP]</b>            FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType, ProxyIp_ProxySetId;  <b>[ProxyIP]</b>            For example:            ProxyIp 0 = 10.33.37.77, -1, 0;            ProxyIp 1 = 10.8.8.10, 0, 2;            ProxyIp 2 = 10.5.6.7, -1, 1;  <b>Notes:</b></p> <ul style="list-style-type: none"> <li>To assign various attributes (such as Proxy Load Balancing) per Proxy Set ID, use the parameter ProxySet.</li> <li>For a description of this table, see 'Configuring Proxy Sets Table' on page 213.</li> </ul>
<b>Proxy Set Table</b>	
Web: Proxy Set Table EMS: Proxy Set CLI: configure voip > control-network proxy-set <b>[ProxySet]</b>	<p>This table parameter configures the Proxy Set ID table. It is used in conjunction with the ProxyIP table ini file parameter, which defines the IP addresses per Proxy Set ID.</p> <p>The ProxySet table ini file parameter defines additional attributes per Proxy Set ID. This includes, for example, Proxy keep-alive and load balancing and redundancy mechanisms (if a Proxy Set contains more than one proxy address).</p> <p>The format of this parameter is as follows:  <b>[ProxySet]</b>            FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD, ProxySet_ClassificationInput, ProxySet_ProxyRedundancyMode;  <b>[ProxySet]</b>            For example:            ProxySet 0 = 0, 60, 0, 0, 0, , 1;            ProxySet 1 = 1, 60, 1, 0, 1, , 0;  <b>Notes:</b></p> <ul style="list-style-type: none"> <li>For configuring the Proxy Set IDs and their IP addresses, use the parameter ProxyIP.</li> <li>For a description of this table, see 'Configuring Proxy Sets Table' on page 213.</li> </ul>
<b>Registrar Parameters</b>	
Web: Enable Registration EMS: Is Register Needed CLI: enable-registration <b>[IsRegisterNeeded]</b>	<p>Enables the device to register to a Proxy/Registrar server.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) The device doesn't register to Proxy/Registrar server.</li> <li><b>[1]</b> Enable = The device registers to Proxy/Registrar server when the device is powered up and at every user-defined interval (configured by the parameter RegistrationTime).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Gateway / IP-to-IP application.</li> <li>The device sends a REGISTER request for each channel or for the entire device (according to the AuthenticationMode parameter).</li> </ul>
Web/EMS: Registrar Name	<p>Defines the Registrar domain name. If specified, the name is used as the Request-URI in REGISTER messages. If isn't specified (default),</p>

Parameter	Description
CLI: registrar-name <b>[RegistrarName]</b>	<p>the Registrar IP address, or Proxy name or IP address is used instead. The valid range is up to 100 characters.</p> <p><b>Note:</b> This parameter is applicable only to the Gateway / IP-to-IP application.</p>
Web: Registrar IP Address EMS: Registrar IP CLI: ip-addr-rgstr <b>[RegistrarIP]</b>	<p>Defines the IP address (or FQDN) and port number (optional) of the Registrar server. The IP address is in dotted-decimal notation, e.g., 201.10.8.1:&lt;5080&gt;.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Gateway / IP-to-IP application.</li> <li>If not specified, the REGISTER request is sent to the primary Proxy server.</li> <li>When a port number is specified, DNS NAPTR/SRV queries aren't performed, even if the parameter DNSQueryType is set to 1 or 2.</li> <li>If the parameter RegistrarIP is set to an FQDN and is resolved to multiple addresses, the device also provides real-time switching (hotswap mode) between different Registrar IP addresses (the parameter IsProxyHotSwap is set to 1). If the first Registrar doesn't respond to the REGISTER message, the same REGISTER message is sent immediately to the next Proxy. To allow this mechanism, the parameter EnableProxyKeepAlive must be set to 0.</li> <li>When a specific transport type is defined using the parameter RegistrarTransportType, a DNS NAPTR query is not performed even if the parameter DNSQueryType is set to 2.</li> </ul>
Web/EMS: Registrar Transport Type CLI: registrar-transport <b>[RegistrarTransportType]</b>	<p>Determines the transport layer used for outgoing SIP dialogs initiated by the device to the Registrar.</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured (default)</li> <li><b>[0]</b> UDP</li> <li><b>[1]</b> TCP</li> <li><b>[2]</b> TLS</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to the Gateway / IP-to-IP application.</li> <li>When set to 'Not Configured', the value of the parameter SIPTransportType is used.</li> </ul>
Web/EMS: Registration Time CLI: registration-time <b>[RegistrationTime]</b>	<p>Defines the time interval (in seconds) for registering to a Proxy server. The value is used in the SIP Expires header. This parameter also defines the time interval between Keep-Alive messages when the parameter EnableProxyKeepAlive is set to 2 (REGISTER). Typically, the device registers every 3,600 sec (i.e., one hour). The device resumes registration according to the parameter RegistrationTimeDivider.</p> <p>The valid range is 10 to 2,000,000. The default is 180.</p>



Parameter	Description
Web: Re-registration Timing [%] EMS: Time Divider CLI: re-registration-timing <b>[RegistrationTimeDivider]</b>	<p>Defines the re-registration timing (in percentage). The timing is a percentage of the re-register timing set by the Registrar server.</p> <p>The valid range is 50 to 100. The default is 50.</p> <p>For example: If this parameter is set to 70% and the Registration Expires time is 3600, the device re-sends its registration request after 3600 x 70% (i.e., 2520 sec).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter may be overridden if the parameter RegistrationTimeThreshold is greater than 0.</li> <li>This parameter is applicable to the GW/IP-to-IP and SBC application.</li> </ul>
Web/EMS: Registration Retry Time CLI: registration-retry-time <b>[RegistrationRetryTime]</b>	<p>Defines the time interval (in seconds) after which a registration request is re-sent if registration fails with a 4xx response or if there is no response from the Proxy/Registrar server.</p> <p>The default is 30 seconds. The range is 10 to 3600.</p>
Web: Registration Time Threshold EMS: Time Threshold CLI: registration-time-thres <b>[RegistrationTimeThreshold]</b>	<p>Defines a threshold (in seconds) for re-registration timing. If this parameter is greater than 0, but lower than the computed re-registration timing (according to the parameter RegistrationTimeDivider), the re-registration timing is set to the following: timing set by the Registration server in the SIP Expires header minus the value of the parameter RegistrationTimeThreshold.</p> <p>The valid range is 0 to 2,000,000. The default is 0.</p>
Web: Re-register On INVITE Failure EMS: Register On Invite Failure CLI: reg-on-invite-fail <b>[RegisterOnInviteFailure]</b>	<p>Enables immediate re-registration if no response is received for an INVITE request sent by the device.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>When enabled, the device immediately expires its re-registration timer and commences re-registration to the same Proxy upon any of the following scenarios:</p> <ul style="list-style-type: none"> <li>The response to an INVITE request is 407 (Proxy Authentication Required) without an authentication header included.</li> <li>The remote SIP UA abandons a call before the device has received any provisional response (indicative of an outbound proxy server failure).</li> <li>The remote SIP UA abandons a call and the only provisional response the device has received for the call is 100 Trying (indicative of a home proxy server failure, i.e., the failure of a proxy in the route after the outbound proxy).</li> <li>The device terminates a call due to the expiration of RFC 3261 Timer B or due to the receipt of a 408 (Request Timeout) response and the device has not received any provisional response for the call (indicative of an outbound proxy server failure).</li> <li>The device terminates a call due to the receipt of a 408 (Request Timeout) response and the only provisional response the device has received for the call is the 100 Trying provisional response (indicative of a home proxy server failure).</li> </ul>
Web: ReRegister On Connection Failure EMS: Re Register On Connection Failure CLI: reg-on-conn-failure	<p>Enables the device to perform SIP re-registration upon TCP/TLS connection failure.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>

Parameter	Description
<b>[ReRegisterOnConnecti onFailure]</b>	
Web: Gateway Registration Name EMS: Name CLI: gw-registration-name <b>[GWRegistrationName]</b>	<p>Defines the user name that is used in the From and To headers in SIP REGISTER messages. If no value is specified (default) for this parameter, the UserName parameter is used instead.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to the Gateway / IP-to-IP application.</li> <li>▪ This parameter is applicable only for single registration per device (i.e., AuthenticationMode is set to 1). When the device registers each channel separately (i.e., AuthenticationMode is set to 0), the user name is set to the channel's phone number.</li> </ul>
Web/EMS: Registration Mode CLI: authentication-mode <b>[AuthenticationMode]</b>	<p>Determines the device's registration and authentication method.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Per Endpoint = Registration and authentication is performed separately for each endpoint/B-channel. This is typically used for FXS interfaces, where each endpoint registers (and authenticates) separately with its user name and password.</li> <li>▪ <b>[1]</b> Per Gateway = (Default) Single registration and authentication for the entire device. This is typically used for FXO interfaces and digital modules.</li> <li>▪ <b>[3]</b> Per FXS = Registration and authentication for FXS endpoints.</li> </ul> <p><b>Note:</b> This parameter is applicable only to the Gateway / IP-to-IP application.</p>
Web: Set Out-Of-Service On Registration Failure EMS: Set OOS On Registration Fail CLI: set-oos-on-reg-failure <b>[OOSOnRegistrationFail ]</b>	<p>Enables setting the endpoint, trunk, or entire device (i.e., all endpoints) to out-of-service if registration fails.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>If the registration is per endpoint (i.e., AuthenticationMode is set to 0) or per Account (see Configuring Hunt Group Settings on page 291) and a specific endpoint/Account registration fails (SIP 4xx or no response), then that endpoint is set to out-of-service until a success response is received in a subsequent registration request. When the registration is per the entire device (i.e., AuthenticationMode is set to 1) and registration fails, all endpoints are set to out-of-service. If all the Accounts of a specific Trunk Group fail registration and if the Trunk Group comprises a complete trunk, then the entire trunk is set to out-of-service.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to the Gateway / IP-to-IP application.</li> <li>▪ The out-of-service method is configured using the FXSOOSBehavior parameter.</li> </ul>
CLI: expl-un-reg <b>[UnregistrationMode]</b>	<p>Enables the device to perform explicit unregisters.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> 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</li> </ul>



Parameter	Description
	<p>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> <p><b>Note:</b> The REGISTER-specific Contact header field value of "*" applies to all registrations, but it can only be used if the Expires header field is present with a value of "0".</p>
Web/EMS: Add Empty Authorization Header CLI: add-empty-author-hdr <b>[EmptyAuthorizationHeader]</b>	<p>Enables the inclusion of the SIP Authorization header in initial registration (REGISTER) requests sent by the device.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>The Authorization header carries the credentials of a user agent (UA) in a request to a server. The sent REGISTER message populates the Authorization header with the following parameters:</p> <ul style="list-style-type: none"> <li>▪ username - set to the value of the private user identity</li> <li>▪ realm - set to the domain name of the home network</li> <li>▪ uri - set to the SIP URI of the domain name of the home network</li> <li>▪ nonce - set to an empty value</li> <li>▪ response - set to an empty value</li> </ul> <p>For example:</p> <pre>Authorization: Digest username=alice_private@home1.net, realm="home1.net", nonce="", response="e56131d19580cd833064787ecc"</pre> <p><b>Note:</b> This registration header is according to the IMS 3GPP TS24.229 and PKT-SP-24.220 specifications.</p>
Web: Add initial Route Header CLI: add-init-rte-hdr <b>[InitialRouteHeader]</b>	<p>Enables the inclusion of the SIP Route header in initial registration or re-registration (REGISTER) requests sent by the device.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>When the device sends a REGISTER message, the Route header includes either the Proxy's FQDN, or IP address and port according to the configured Proxy Set, for example:</p> <pre>Route: &lt;sip:10.10.10.10;lr;transport=udp&gt;</pre> <p>or</p> <pre>Route: &lt;sip: pcscf-gm.ims.rr.com;lr;transport=udp&gt;</pre>
EMS: Ping Pong Keep Alive <b>[UsePingPongKeepAlive]</b>	<p>Enables the use of the carriage-return and line-feed sequences (CRLF) Keep-Alive mechanism, according to RFC 5626 "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)" for reliable, connection-orientated transport types such as TCP.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>The SIP user agent/client (i.e., device) uses a simple periodic message as a keep-alive mechanism to keep their flow to the proxy or registrar alive (used for example, to keep NAT bindings open). For connection-oriented transports such as TCP/TLS this is based on CRLF. This mechanism uses a client-to-server "ping" keep-alive and a corresponding server-to-client "pong" message. This ping-pong</p>

Parameter	Description
	<p>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><b>Note:</b> The device sends a CRLF message to the Proxy Set only if the Proxy Keep-Alive feature (EnableProxyKeepAlive parameter) is enabled and its transport type is set to TCP or TLS. The device first sends a SIP OPTION message to establish the TCP/TLS connection and if it receives any SIP response, it continues sending the CRLF keep-alive sequences.</p>
EMS: Ping Pong Keep Alive Time [PingPongKeepAliveTime]	<p>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.</p> <p>The default range is 5 to 2,000,000. The default is 120.</p> <p>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.</p>

## 59.7.2 Network Application Parameters

The SIP network application parameters are described in the table below.

**SIP Network Application Parameters**

Parameter	Description
<b>Signaling Routing Domain Table</b>	
Web: SRD Settings EMS: SRD Table CLI: configure voip > control-network srd [SRD]	<p>This table parameter configures the Signaling Routing Domain (SRD) table. The format of this parameter is as follows:</p> <p><b>[SRD]</b>  FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations;  <b>[SRD]</b></p> <p>For example:  SRD 1 = LAN1_SRD, Mrealm1, 0, 1, 15, 1;  SRD 2 = LAN2_SRD, Mrealm2, 0, 1, 15, 1;</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring SRD Table' on page 199.</p>
<b>SIP Interface Table</b>	
Web: SIP Interface Table EMS: SIP Interfaces Table CLI: configure voip > control-network sip-	<p>This table parameter configures the SIP Interface table. The SIP Interface represents a SIP signaling entity, comprising ports (UDP, TCP, and TLS) and associated with a specific IP interface and an SRD ID. The format of this parameter is as follows:</p>

Parameter	Description
interface <b>[SIPInterface]</b>	<p>[SIPInterface]            FORMAT SIPInterface_Index = SIPInterface_NetworkInterface,            SIPInterface_ApplicationType, SIPInterface_UDPPort,            SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRD,            SIPInterface_MessagePolicy, SIPInterface_TLSMutualAuthentication,            SIPInterface_TCPKeepaliveEnable,            SIPInterface_ClassificationFailureResponseType;            [SIPInterface]</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring SIP Interface Table' on page 201.</p>
TCP Keep Alive Idle Time <b>[TCPKeepAliveTime]</b>	<p>Defines the interval (in sec) between the last data packet sent and the first keep-alive probe to send.            The valid value is 10 to 65,000. The default is 60.</p> <p>Notes:</p> <ul style="list-style-type: none"> <li>Simple ACKs such as keep-alives are not considered data packets.</li> <li>TCP keepalive is enabled per SIP Interface in the SIP Interface table.</li> </ul>
TCP Keep Alive Interval Time <b>[TCPKeepAliveInterval]</b>	<p>Defines the interval (in sec) between consecutive keep-alive probes, regardless of what the connection has exchanged in the meantime.            The valid value is 10 to 65,000. The default is 10.</p> <p><b>Note:</b> TCP keepalive is enabled per SIP Interface in the SIP Interface table.</p>
TCP Keep Alive Retry Number <b>[TCPKeepAliveRetry]</b>	<p>Defines the number of unacknowledged keep-alive probes to send before considering the connection down.            The valid value is 1 to 100. The default is 5.</p> <p><b>Note:</b> TCP keepalive is enabled per SIP Interface in the SIP Interface table.</p>
<b>NAT Translation Table</b>	
Web: NAT Translation Table CLI: configure voip > control-network NATTranslation <b>[NATTranslation]</b>	<p>This table parameter defines NAT rules for translating source IP addresses per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses. This allows, for example, the separation of VoIP traffic between different ISTP's, and topology hiding (of internal IP addresses to the "public" network). Each IP interface (configured in the Multiple Interface table - InterfaceTable parameter) can be associated with a NAT rule in this table, translating the source IP address and port of the outgoing packet into the NAT address (IP address and port range).</p> <p>The format of this parameter is as follows:</p> <p><b>[ NATTranslation ]</b>            FORMAT NATTranslation_Index =            NATTranslation_SourceIPInterfaceName,            NATTranslation_TargetIPAddress, NATTranslation_SourceStartPort,            NATTranslation_SourceEndPort, NATTranslation_TargetStartPort,            NATTranslation_TargetEndPort;            [ NATTranslation ]</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring NAT Translation per IP Interface' on page 127.</p>

## 59.8 General SIP Parameters

The general SIP parameters are described in the table below.

**General SIP Parameters**

Parameter	Description
Web: SIP Remote Reset CLI: sip-remote-reset <b>[EnableSIPRemoteReset]</b>	<p>Enables a specific device action upon the receipt of a SIP NOTIFY request, where the action depends on the value received in the Event header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>The action depends on the Event header value:</p> <ul style="list-style-type: none"> <li>'check-sync;reboot=false': triggers the regular Automatic Update feature (if Automatic Update has been enabled on the device)</li> <li>'check-sync;reboot=true': triggers a device reset</li> </ul> <p><b>Note:</b> The Event header value is proprietary to AudioCodes.</p>
Web/EMS: Max SIP Message Length <b>[KB]</b> <b>[MaxSIPMessageLength]</b>	<p>Defines the maximum size (in Kbytes) for each SIP message that can be sent over the network. The device rejects messages exceeding this user-defined size.</p> <p>The valid value range is 1 to 50. The default is 50.</p>
<b>[SIPForceRport]</b>	<p>Determines whether the device sends SIP responses to the UDP port from where SIP requests are received even if the 'rport' parameter is not present in the SIP Via header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disabled. The device sends the SIP response to the UDP port defined in the Via header. If the Via header contains the 'rport' parameter, the response is sent to the UDP port from where the SIP request is received.</li> <li><b>[1]</b> = Enabled. SIP responses are sent to the UDP port from where SIP requests are received even if the 'rport' parameter is not present in the Via header.</li> </ul>
Web: Reject Cancel after Connect CLI: reject-cancel-after-connect <b>[RejectCancelAfterConnect]</b>	<p>Determines whether the device accepts or rejects a SIP CANCEL request received after the receipt of a 200 OK, during an established call.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Accepts the CANCEL, by responding with a 200 OK and terminating the call session.</li> <li><b>[1]</b> = Rejects the CANCEL, by responding with a SIP 481 Call/Transaction Does Not Exist, and maintaining the call session.</li> </ul>
Web: Verify Received RequestURI CLI: verify-rcvd-requri <b>[VerifyReceivedRequestUri]</b>	<p>Enables the device to reject SIP requests (such as ACK, BYE, or re-INVITE) whose user part in the Request-URI is different from the user part received in the Contact header of the last sent SIP request.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Even if the user is different, the device accepts the SIP request.</li> <li><b>[1]</b> Enable = If the user is different, the device rejects the SIP request (BYE is responded with 481; re-INVITE is responded with 404; ACK is ignored).</li> </ul>
Web: Max Number of Active Calls EMS: Maximum Concurrent Calls CLI: max-nb-of--act-calls <b>[MaxActiveCalls]</b>	<p>Defines the maximum number of simultaneous active calls supported by the device. If the maximum number of calls is reached, new calls are not established.</p> <p>The valid range is 1 to the maximum number of supported channels.</p> <p>The default value is the maximum available channels (i.e., no restriction on the maximum number of calls).</p>

Parameter	Description
Web: Number of Calls Limit <b>[CallLimit]</b>	<p>Defines the maximum number of concurrent calls per IP Profile. If the IP Profile is set to some limit, the device maintains the number of concurrent calls (incoming and outgoing) pertaining to the specific profile. When the number of concurrent calls is equal to the limit, the device rejects any new incoming and outgoing calls belonging to that profile.</p> <p>This parameter can also be set to the following:</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> = (Default) There is no limitation on calls for that IP Profile.</li> <li>▪ <b>[0]</b> = Calls are rejected.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter can only be configured for an IP Profile using the IPProfile parameter (see 'Configuring IP Profiles' on page 239).</li> <li>▪ For IP-to-IP calls, you can configure the device to route calls to an alternative IP Group when the maximum number of concurrent calls is reached. To do so, you need to add an alternative routing rule in the Outbound IP Routing table that reroutes the call to an alternative IP Group. You also need to add a rule to the Reason for Alternative Routing table to initiate an alternative rule for Tel-to-IP calls using cause 805.</li> </ul>
Web: QoS statistics in SIP Release Call <b>[QoSStatistics]</b>	<p>Enables the device to include call quality of service (QoS) statistics in SIP BYE and SIP 200 OK response to BYE, using the proprietary SIP header X-RTP-Stat.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul> <p>The X-RTP-Stat header provides the following statistics:</p> <ul style="list-style-type: none"> <li>▪ Number of received and sent voice packets</li> <li>▪ Number of received and sent voice octets</li> <li>▪ Received packet loss, jitter (in ms), and latency (in ms)</li> </ul> <p>The X-RTP-Stat header contains the following fields:</p> <ul style="list-style-type: none"> <li>▪ PS=&lt;voice packets sent&gt;</li> <li>▪ OS=&lt;voice octets sent&gt;</li> <li>▪ PR=&lt;voice packets received&gt;</li> <li>▪ OR=&lt;voice octets received&gt;</li> <li>▪ PL=&lt;receive packet loss&gt;</li> <li>▪ JI=&lt;jitter in ms&gt;</li> <li>▪ LA=&lt;latency in ms&gt;</li> </ul> <p>Below is an example of the X-RTP-Stat header in a SIP BYE message:</p> <pre> BYE sip:302@10.33.4.125 SIP/2.0 Via: SIP/2.0/UDP 10.33.4.126;branch=z9hG4bKac2127550866 Max-Forwards: 70 From: &lt;sip:401@10.33.4.126;user=phone&gt;;tag=1c2113553324 To: &lt;sip:302@company.com&gt;;tag=1c991751121 Call-ID: 991750671245200001912@10.33.4.125 CSeq: 1 BYE <b>X-RTP-Stat:</b> <b>PS=207;OS=49680;;PR=314;OR=50240;PL=0;JI=600;LA=40;</b> Supported: em,timer,replaces,path,resource-priority           </pre>

Parameter	Description
	<p>Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE, UPDATE</p> <p>User-Agent: Sip-Gateway-/v.6.2A.008.006</p> <p>Reason: Q.850 ;cause=16 ;text="local"</p> <p>Content-Length: 0</p>
Web/EMS: PRACK Mode CLI: prack-mode <b>[PrackMode]</b>	<p>Determines the PRACK (Provisional Acknowledgment) mechanism mode for SIP 1xx reliable responses.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable</li> <li>▪ <b>[1]</b> Supported (default)</li> <li>▪ <b>[2]</b> Required</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The Supported and Required headers contain the '100rel' tag.</li> <li>▪ The device sends PRACK messages if 180/183 responses are received with '100rel' in the Supported or Required headers.</li> </ul>
Web/EMS: Enable Early Media CLI: early-media <b>[EnableEarlyMedia]</b>	<p>Enables the Early Media feature.</p> <p>Digital: Enables the device to send a 18x response with SDP instead of a 18x, allowing the media stream to be established prior to the answering of the call.</p> <p>Analog: Enables the device to send a 183 Session Progress response with SDP instead of a 180 Ringing, allowing the media stream to be established prior to the answering of the call.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>Digital: The inclusion of the SDP in the 18x response depends on the ISDN Progress Indicator (PI). The SDP is sent only if PI is set to 1 or 8 in the received Proceeding, Alerting, or Progress PRI messages. See also the ProgressIndicator2IP parameter, which if set to 1 or 8, the device behaves as if it received the ISDN messages with the PI.</p> <ul style="list-style-type: none"> <li>▪ For the CAS protocol: See the ProgressIndicator2IP parameter.</li> <li>▪ For the ISDN protocol: Sending a 183 response depends on the ISDN PI. It is sent only if PI is set to 1 or 8 in the received Proceeding or Alerting PRI messages. Sending 183 response also depends on the ReleaseIP2ISDNCallOnProgressWithCause parameter, which must be set to any value except 2.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ See also the IgnoreAlertAfterEarlyMedia parameter. This parameter allows, for example, to interwork Alert + PI to SIP 183 + SDP instead of 180 + SDP.</li> <li>▪ You can also configure early SIP 183 response immediately upon receipt of an INVITE, using the EnableEarly183 parameter.</li> <li>▪ Analog: To send a 183 response, you must also set the parameter ProgressIndicator2IP to 1. If it is equal to 0, 180 Ringing response is sent.</li> <li>▪ This feature can also be configured as an IP Profile and/or Tel Profile.</li> <li>▪ This parameter is applicable only to the Gateway/IP-to-IP application.</li> </ul>
Web/EMS: Enable Early 183 CLI: early-183	<p>Enables the device to send SIP 183 responses with SDP to the IP upon receipt of INVITE messages. This parameter is applicable to IP-to-Tel (ISDN) and IP-to-IP calls, and applies to all calls.</p>



Parameter	Description
<b>[EnableEarly183]</b>	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable <ul style="list-style-type: none"> <li>✓ IP-to-Tel calls: By sending the 183 response, the device opens an RTP channel before receiving the "progress" tone from the ISDN side. The device sends RTP packets immediately upon receipt of an ISDN Progress, Alerting with Progress indicator, or Connect message according to the initial negotiation without sending the 183 response again, thereby saving response time and avoiding early media clipping.</li> <li>✓ IP-to-IP calls: Sending the 183 response enables SIP servers that require a stream of early media, to keep sessions open.</li> </ul> </li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To enable this feature, set the EnableEarlyMedia parameter to 1.</li> <li>▪ When the BChannelNegotiation parameter is set to a non-Exclusive value (Preferred or Any), the EnableEarly183 parameter is ignored and a SIP 183 is not sent upon receipt of an INVITE. In such a case, you can set the ProgressIndicator2IP parameter to 1 (PI = 1) for the device to send a SIP 183 upon receipt of an ISDN Call Proceeding message.</li> <li>▪ This feature can also be configured in an IP Profile.</li> </ul>
<b>[IgnoreAlertAfterEarlyMedia]</b>	<p>Determines the device's interworking of Alerting messages from PRI to SIP.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disabled (default)</li> <li>▪ <b>[1]</b> = Enabled</li> </ul> <p>When enabled, if the device sends a 183 response with an SDP (due to a received ISDN Progress or Proceeding with PI messages) and an Alerting message is then received from the Tel side (with or without Progress Indicator), the device does not send an additional 18x response, and the voice channel remains open. However, if the device did not send a 183 with an SDP and it receives an Alert without PI, the device sends a 180 (without SDP). If it receives an Alert with PI it sends a 183 with an SDP.</p> <p>When disabled, the device sends additional 18x responses as a result of receiving Alerting and Progress messages, regardless of whether or not a 18x response was already sent.</p> <p><b>Note:</b> This parameter is applicable only if the EnableEarlyMedia parameter is set to 1 (i.e., enabled).</p>
Web: 183 Message Behavior EMS: SIP 183 Behaviour CLI: 183-msg-behavior <b>[SIP183Behaviour]</b>	<p>Digital: Defines the ISDN message that is sent when the 183 Session Progress message is received for IP-to-Tel calls. Analog: Defines the response of the device upon receipt of a SIP 183 response.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Progress = (Default) Digital: The device sends a Progress message. Analog: A 183 response (without SDP) does not cause the device to play a ringback tone.</li> <li>▪ <b>[1]</b> Alert = Digital: The device sends an Alerting message (upon receipt of a 183 response) instead of an ISDN Progress message. Analog: 183 response is handled by the device as if a 180 Ringing response is received, and the device plays a ringback tone.</li> </ul>
<b>[ReleaseIP2ISDNCallOnProgressWithCause]</b>	<p>Typically, if an Q.931 Progress message with a Cause is received from the PSTN for an outgoing IP-to-ISDN call and the EnableEarlyMedia parameter is set to 1 (i.e., the Early Media feature is enabled), the device interworks the Progress to 183 + SDP to enable the originating party to hear the PSTN announcement about the call failure.</p>

Parameter	Description
	<p>Conversely, if EnableEarlyMedia is set to 0, the device disconnects the call by sending a SIP 4xx response to the originating party. However, if the ReleaseIP2ISDNCallOnProgressWithCause parameter is set to 1, then the device sends a SIP 4xx response even if the EnableEarlyMedia parameter is set to 1.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) If a Progress with Cause message is received from the PSTN for an outgoing IP-to-ISDN call, the device does not disconnect the call by sending a SIP 4xx response to the originating party.</li> <li>▪ <b>[1]</b> = The device sends a SIP 4xx response when the EnableEarlyMedia parameter is set to 0.</li> <li>▪ <b>[2]</b> = The device always sends a SIP 4xx response, even if the EnableEarlyMedia parameter is set to 1.</li> </ul>
Web: Session-Expires Time EMS: Sip Session Expires CLI: session-expires-time <b>[SIPSessionExpires]</b>	<p>Defines the numerical value sent in the Session-Expires header in the first INVITE request or response (if the call is answered).</p> <p>The valid range is 1 to 86,400 sec. The default is 0 (i.e., the Session-Expires header is disabled).</p>
Web: Minimum Session-Expires EMS: Minimal Session Refresh Value CLI: min-session-expires <b>[MinSE]</b>	<p>Defines the time (in seconds) that is used in the Min-SE header. This header defines the minimum time that the user agent refreshes the session.</p> <p>The valid range is 10 to 100,000. The default is 90.</p>
Web/EMS: Session Expires Disconnect Time CLI: session-exp-disconnect-time <b>[SessionExpiresDisconnectTime]</b>	<p>Defines a session expiry timeout. The device disconnects the session (sends a SIP BYE) if the refresher did not send a refresh request before one-third (1/3) of the session expires time, or before the time configured by this parameter (the minimum of the two).</p> <p>The valid range is 0 to 32 (in seconds). The default is 32.</p>
Web/EMS: Session Expires Method CLI: session-exp-method <b>[SessionExpiresMethod]</b>	<p>Determines the SIP method used for session-timer updates.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Re-INVITE = (Default) Uses Re-INVITE messages for session-timer updates.</li> <li>▪ <b>[1]</b> UPDATE = Uses UPDATE messages.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The device can receive session-timer refreshes using both methods.</li> <li>▪ The UPDATE message used for session-timer is excluded from the SDP body.</li> </ul>
<b>[RemoveToTagInFailureResponse]</b>	<p>Determines whether the device removes the 'to' header tag from final SIP failure responses to INVITE transactions.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Do not remove tag.</li> <li>▪ <b>[1]</b> = Remove tag.</li> </ul>
<b>[EnableRTCPAttribute]</b>	<p>Enables the use of the 'rtcp' attribute in the outgoing SDP.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul> <p><b>Note:</b> This parameter is applicable only to the IP-to-IP/GW application.</p>
EMS: Options User Part <b>[OPTIONSUserPart]</b>	<p>Defines the user part value of the Request-URI for outgoing SIP OPTIONS requests. If no value is configured, the endpoint number (analog) or configuration parameter 'Username' value (digital) is used. A special value is 'empty', indicating that no user part in the Request-</p>



Parameter	Description
	<p>URI (host part only) is used.</p> <p>The valid range is a 30-character string. The default value is an empty string ("").</p>
Web: TDM Over IP Minimum Calls For Trunk Activation EMS: TDM Over IP Min Calls For Trunk Activation <b>[TDMOverIPMinCallsForTrunkActivation]</b>	<p>Defines the minimal number of SIP dialogs that must be established when using TDM Tunneling to consider the specific trunk as active.</p> <p>When using TDM Tunneling, if calls from this defined number of B-channels pertaining to a specific Trunk fail (i.e., SIP dialogs are not correctly set up), an AIS alarm is sent on this trunk toward the PSTN and all current calls are dropped. The originator gateway continues the INVITE attempts. When this number of calls succeed (i.e., SIP dialogs are correctly set up), the AIS alarm is cleared.</p> <p>The valid range is 0 to 31. The default is 0 (i.e., don't send AIS alarms).</p>
<b>[TDMolPInitiateInviteTime]</b>	<p>Defines the time (in msec) between the first INVITE issued within the same trunk when implementing the TDM tunneling application.</p> <p>The valid value range is 500 to 1000. The default is 2000.</p>
<b>[TDMolPInviteRetryTime]</b>	<p>Defines the time (in msec) between call release and a new INVITE when implementing the TDM tunneling application.</p> <p>The valid value range is 10,000 to 20,000. The default is 10,000.</p>
Web: Fax Signaling Method EMS: Fax Used CLI: fax-sig-method <b>[IsFaxUsed]</b>	<p>Determines the SIP signaling method for establishing and transmitting a fax session after a fax is detected.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No Fax = (Default) No fax negotiation using SIP signaling. Fax transport method is according to the parameter FaxTransportMode.</li> <li>▪ <b>[1]</b> T.38 Relay = Initiates T.38 fax relay.</li> <li>▪ <b>[2]</b> G.711 Transport = Initiates fax/modem using the coder G.711 A-law/Mu-law with adaptations (see Note below).</li> <li>▪ <b>[3]</b> Fax Fallback = Initiates T.38 fax relay. If the T.38 negotiation fails, the device re-initiates a fax session using the coder G.711 A-law/<math>\mu</math>-law with adaptations (see the Note below).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ Fax adaptations (for options 2 and 3):               <ul style="list-style-type: none"> <li>✓ Echo Celler = On</li> <li>✓ Silence Compression = Off</li> <li>✓ Echo Celler Non-Linear Processor Mode = Off</li> <li>✓ Dynamic Jitter Buffer Minimum Delay = 40</li> <li>✓ Dynamic Jitter Buffer Optimization Factor = 13</li> </ul> </li> <li>▪ If the device initiates a fax session using G.711 (option 2 and possibly 3), a 'gpmid' attribute is added to the SDP in the following format:               <ul style="list-style-type: none"> <li>✓ <b>For A-law:</b> 'a=gpmid:8 vbd=yes;ecan=on'</li> <li>✓ <b>For <math>\mu</math>-law:</b> 'a=gpmid:0 vbd=yes;ecan=on'</li> </ul> </li> <li>▪ When this parameter is set to 1, 2, or 3, the parameter FaxTransportMode is ignored.</li> <li>▪ When this parameter is set to 0, T.38 might still be used without the control protocol's involvement. To completely disable T.38, set FaxTransportMode to a value other than 1.</li> <li>▪ This parameter can also be configured per IP Profile (using the IPProfile parameter).</li> <li>▪ For more information on fax transport methods, see 'Fax/Modem Transport Modes' on page 149.</li> </ul>

Parameter	Description
<b>[HandleG711asVBD]</b>	<p>Enables the handling of G.711 as G.711 Voice Band Data (VBD) coder.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disable. The device negotiates G.711 as a regular audio coder and sends an answer only with G.729 coder. For example, if the device is configured with G.729 and G.711 VBD coders and it receives an INVITE with an SDP offer containing G.729 and “regular” G.711 coders, it sends an SDP answer containing only the G.729 coder.</li> <li><b>[1]</b> = Enable. The device assumes that the G.711 coder received in the INVITE SDP offer is a VBD coder. For example, if the device is configured with G.729 and G.711 VBD coders and it receives an INVITE with an SDP offer containing G.729 and “regular” G.711 coders, it sends an SDP answer containing G.729 and G.711 VBD coders, allowing a subsequent bypass (passthrough) session if fax/modem signals are detected during the call.</li> </ul> <p><b>Note:</b> This parameter is applicable only if G.711 VBD coder(s) with regular G.711 payload types 0 or 8 are configured for the device (using the CodersGroup parameter).</p>
CLI: fax-vbd-behvr <b>[FaxVBDBehavior]</b>	<p>Determines the device's fax transport behavior when G.711 VBD coder is negotiated at call start.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) If the device is configured with a VBD coder (see the CodersGroup parameter) and is negotiated OK at call start, then both fax and modem signals are sent over RTP using the bypass payload type (and no mid-call VBD or T.38 Re-INVITES occur).</li> <li><b>[1]</b> = If the IsFaxUsed parameter is set to 1, the channel opens with the FaxTransportMode parameter set to 1 (relay). This is required to detect mid-call fax tones and to send T.38 Re-INVITE messages upon fax detection. If the remote party supports T.38, the fax is relayed over T.38.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If VBD coder negotiation fails at call start and if the IsFaxUsed parameter is set to 1 (or 3), then the channel opens with the FaxTransportMode parameter set to 1 (relay) to allow future detection of fax tones and sending of T.38 Re-INVITES. In such a scenario, the FaxVBDBehavior parameter has no effect.</li> <li>This feature can be used only if the remote party supports T.38 fax relay; otherwise, the fax fails.</li> </ul>
<b>[NoAudioPayloadType]</b>	<p>Defines the payload type of the outgoing SDP offer.</p> <p>The valid value range is 96 to 127 (dynamic payload type). The default is 0 (i.e. NoAudio is not supported). For example, if set to 120, the following is added to the INVITE SDP:</p> <pre>a=rtpmap:120 NoAudio/8000\r\n</pre> <p><b>Note:</b> For incoming SDP offers, NoAudio is always supported.</p>
Web: SIP Transport Type EMS: Transport Type CLI: app-sip-transport-type <b>[SIPTransportType]</b>	<p>Determines the default transport layer for outgoing SIP calls initiated by the device.</p> <ul style="list-style-type: none"> <li><b>[0]</b> UDP (default)</li> <li><b>[1]</b> TCP</li> <li><b>[2]</b> TLS (SIPS)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>It's recommended to use TLS for communication with a SIP Proxy and not for direct device-to-device communication.</li> <li>For received calls (i.e., incoming), the device accepts all these</li> </ul>

Parameter	Description
	<p>protocols.</p> <ul style="list-style-type: none"> <li>The value of this parameter is also used by the SAS application as the default transport layer for outgoing SIP calls.</li> </ul>
Web: SIP UDP Local Port EMS: Local SIP Port CLI: sip-udp-local-port <b>[LocalSIPPort]</b>	Defines the local UDP port for SIP messages. The valid range is 1 to 65534. The default is 5060.
Web: SIP TCP Local Port EMS: TCP Local SIP Port CLI: sip-tcp-local-port <b>[TCPLocalSIPPort]</b>	Defines the local TCP port for SIP messages. The valid range is 1 to 65535. The default is 5060.
Web: SIP TLS Local Port EMS: TLS Local SIP Port CLI: sip-tls-local-port <b>[TLSTLocalSIPPort]</b>	Defines the local TLS port for SIP messages. The valid range is 1 to 65535. The default is 5061. <b>Note:</b> The value of this parameter must be different from the value of the parameter TCPLocalSIPPort.
Web/EMS: Enable SIPS CLI: enable-sips <b>[EnableSIPS]</b>	Enables secured SIP (SIPS URI) connections over multiple hops. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> 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). <b>Note:</b> If this parameter is enabled and the parameter SIPTransportType is set to 0 (i.e., UDP), the connection fails.
Web/EMS: Enable TCP Connection Reuse CLI: tcp-conn-reuse <b>[EnableTCPConnectionReuse]</b>	Enables the reuse of the same TCP connection for all calls to the same destination. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Uses a separate TCP connection for each call.</li> <li><b>[1]</b> Enable = (Default) Uses the same TCP connection for all calls.</li> </ul> <b>Note:</b> For the SAS application, this feature is configured using the SASConnectionReuse parameter.
Web: Fake TCP alias CLI: fake-tcp-alias <b>[FakeTCPalias]</b>	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. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) TCP/TLS connection reuse is done only if the "alias" parameter is present in the Via header of the first INVITE.</li> <li><b>[1]</b> Enable</li> </ul> <b>Note:</b> To enable TCP/TLS connection re-use, set the EnableTCPConnectionReuse parameter to 1.
Web/EMS: Reliable Connection Persistent Mode CLI: reliable-conn-persistent <b>[ReliableConnectionPersistentMode]</b>	Enables setting of all TCP/TLS connections as persistent and therefore, not released. <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disable. All TCP connections (except those that are set to a proxy IP) are released if not used by any SIP dialog\transaction.</li> <li><b>[1]</b> = Enable - TCP connections to all destinations are persistent and not released unless the device reaches 70% of its maximum TCP resources.</li> </ul> While trying to send a SIP message connection, reuse policy determines whether live connections to the specific destination are re-

Parameter	Description
	<p>used.</p> <p>Persistent TCP connection ensures less network traffic due to fewer setting up and tearing down of TCP connections and reduced latency on subsequent requests due to avoidance of initial TCP handshake. For TLS, persistent connection may reduce the number of costly TLS handshakes to establish security associations, in addition to the initial TCP connection set up.</p> <p><b>Note:</b> If the destination is a Proxy server, the TCP/TLS connection is persistent regardless of the settings of this parameter.</p>
Web/EMS: TCP Timeout CLI: tcp-timeout <b>[SIPTCPTimeout]</b>	<p>Defines the Timer B (INVITE transaction timeout timer) and Timer F (non-INVITE transaction timeout timer), as defined in RFC 3261, when the SIP Transport Type is TCP.</p> <p>The valid range is 0 to 40 sec. The default is 64 multiplied by the SipT1Rtx parameter value. For example, if SipT1Rtx is set to 500 msec, then the default of SIPTCPTimeout is 32 sec.</p>
Web: SIP Destination Port EMS: Destination Port CLI: sip-dst-port <b>[SIPDestinationPort]</b>	<p>Defines the SIP destination port for sending initial SIP requests.</p> <p>The valid range is 1 to 65534. The default port is 5060.</p> <p><b>Note:</b> SIP responses are sent to the port specified in the Via header.</p>
Web: Use user=phone in SIP URL EMS: Is User Phone CLI: user=phone-in-url <b>[IsUserPhone]</b>	<p>Determines whether the 'user=phone' string is added to the SIP URI and SIP To header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = 'user=phone' string is not added.</li> <li><b>[1]</b> Yes = (Default) 'user=phone' string is part of the SIP URI and SIP To header.</li> </ul>
Web: Use user=phone in From Header EMS: Is User Phone In From CLI: phone-in-from-hdr <b>[IsUserPhoneInFrom]</b>	<p>Determines whether the 'user=phone' string is added to the From and Contact SIP headers.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) Doesn't add 'user=phone' string.</li> <li><b>[1]</b> Yes = 'user=phone' string is part of the From and Contact headers.</li> </ul>
Web: Use Tel URI for Asserted Identity CLI: uri-for-assert-id <b>[UseTelURIForAssertedID]</b>	<p>Determines the format of the URI in the P-Asserted-Identity and P-Preferred-Identity headers.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) 'sip:'</li> <li><b>[1]</b> Enable = 'tel:'</li> </ul>
Web: Tel to IP No Answer Timeout EMS: IP Alert Timeout CLI: tel2ip-no-ans-timeout <b>[IPAlertTimeout]</b>	<p>Defines the time (in seconds) that the device waits for a 200 OK response from the called party (IP side) after sending an INVITE message. If the timer expires, the call is released.</p> <p>The valid range is 0 to 3600. The default is 180.</p>
Web: Enable Remote Party ID EMS: Enable RPI Header CLI: remote-party-id <b>[EnableRPIheader]</b>	<p>Enables Remote-Party-Identity headers for calling and called numbers for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> Enable = Remote-Party-Identity headers are generated in SIP INVITE messages for both called and calling numbers.</li> </ul>
Web: Enable History-Info Header EMS: Enable History Info CLI: hist-info-hdr <b>[EnableHistoryInfo]</b>	<p>Enables usage of the History-Info header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>User Agent Client (UAC) Behavior:</b></p> <ul style="list-style-type: none"> <li>Initial request: The History-Info header is equal to the Request-URI.</li> </ul>

Parameter	Description											
	<p>If a PSTN Redirect number is received, it is added as an additional History-Info header with an appropriate reason.</p> <ul style="list-style-type: none"> <li>Upon receiving the final failure response, the device copies the History-Info as is, adds the reason of the failure response to the last entry, and concatenates a new destination to it (if an additional request is sent). The order of the reasons is as follows: <ul style="list-style-type: none"> <li>c. Q.850 Reason</li> <li>d. SIP Reason</li> <li>e. SIP Response code</li> </ul> </li> <li>Upon receiving the final response (success or failure), the device searches for a Redirect reason in the History-Info (i.e., 3xx/4xx SIP reason). If found, it is passed to ISDN according to the following table:</li> </ul> <table border="1"> <thead> <tr> <th>SIP Reason Code</th><th>ISDN Redirecting Reason</th></tr> </thead> <tbody> <tr> <td>302 - Moved Temporarily</td><td>Call Forward Universal (CFU)</td></tr> <tr> <td>408 - Request Timeout</td><td rowspan="3">Call Forward No Answer (CFNA)</td></tr> <tr> <td>480 - Temporarily Unavailable</td></tr> <tr> <td>487 - Request Terminated</td></tr> <tr> <td>486 - Busy Here</td><td rowspan="2">Call Forward Busy (CFB)</td></tr> <tr> <td>600 - Busy Everywhere</td></tr> </tbody> </table> <ul style="list-style-type: none"> <li>If history reason is a Q.850 reason, it is translated to the SIP reason (according to the SIP-ISDN tables) and then to ISDN Redirect reason according to the table above.</li> </ul> <p><b>User Agent Server (UAS) Behavior:</b></p> <ul style="list-style-type: none"> <li>The History-Info header is sent only in the final response.</li> <li>Upon receiving a request with History-Info, the UAS checks the policy in the request. If a 'session', 'header', or 'history' policy tag is found, the (final) response is sent without History-Info; otherwise, it is copied from the request.</li> </ul>	SIP Reason Code	ISDN Redirecting Reason	302 - Moved Temporarily	Call Forward Universal (CFU)	408 - Request Timeout	Call Forward No Answer (CFNA)	480 - Temporarily Unavailable	487 - Request Terminated	486 - Busy Here	Call Forward Busy (CFB)	600 - Busy Everywhere
SIP Reason Code	ISDN Redirecting Reason											
302 - Moved Temporarily	Call Forward Universal (CFU)											
408 - Request Timeout	Call Forward No Answer (CFNA)											
480 - Temporarily Unavailable												
487 - Request Terminated												
486 - Busy Here	Call Forward Busy (CFB)											
600 - Busy Everywhere												
Web: Use Tgrp Information EMS: Use SIP Tgrp CLI: use-tgrp-inf <b>[UseSIP Tgrp]</b>	<p>Determines whether the SIP 'tgrp' parameter is used. This SIP parameter specifies the Trunk Group to which the call belongs (according to RFC 4904). For example, the SIP message below indicates that the call belongs to Trunk Group ID 1:</p> <pre>INVITE sip:+16305550100;tgrp=1;trunk-context=example.com@10.1.0.3;user=phone SIP/2.0</pre> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) The 'tgrp' parameter isn't used.</li> <li><b>[1]</b> Send Only = The Trunk Group number or name (configured in the Hunt Group Settings) is added to the 'tgrp' parameter value in the Contact header of outgoing SIP messages. If a Trunk Group number / name is not associated with the call, the 'tgrp' parameter isn't included. If a 'tgrp' value is specified in incoming messages, it is ignored.</li> <li><b>[2]</b> Send and Receive = The functionality of outgoing SIP messages is identical to the functionality described for option <b>[1]</b>. In addition, for incoming SIP INVITES, if the Request-URI includes a 'tgrp' parameter, the device routes the call according to that value (if possible). The Contact header in the outgoing SIP INVITE (Tel-to-IP call) contains "tgrp=&lt;source trunk group ID&gt;;trunk-context=&lt;gateway IP address&gt;". The &lt;source trunk group ID&gt; is the Trunk Group ID where incoming calls from Tel is received. For IP-Tel calls, the SIP</li> </ul>											

Parameter	Description
	<p>200 OK device's response contains "tgrp=&lt;destination trunk group ID&gt;;trunk-context=&lt;gateway IP address&gt;". The &lt;destination trunk group ID&gt; is the Trunk Group ID used for outgoing Tel calls. The &lt;gateway IP address&gt; in "trunk-context" can be configured using the SIPGatewayName parameter.</p> <ul style="list-style-type: none"> <li><b>[3] Hotline</b> = Interworks the hotline "Off Hook Indicator" parameter between SIP and ISDN: <ul style="list-style-type: none"> <li>✓ For IP-to-ISDN calls: <ul style="list-style-type: none"> <li>- The device interworks the SIP tgrp=hotline parameter (received in INVITE) to ISDN Setup with the Off Hook Indicator IE of "Voice", and "Speech" Bearer Capability IE. Note that the Off Hook Indicator IE is described in UCR 2008 specifications.</li> <li>- The device interworks the SIP tgrp=hotline-ccdata parameter (received in INVITE) to ISDN Setup with an Off Hook Indicator IE of "Data", and with "Unrestricted 64k" Bearer Capability IE. The following is an example of the INVITE with tgrp=hotline-ccdata:</li> </ul> </li> </ul> </li> </ul> <pre>INVITE sip:1234567;tgrp=hotline-ccdata;trunk-context=dsn.mil@example.com</pre> <ul style="list-style-type: none"> <li>✓ For ISDN-to-IP calls: <ul style="list-style-type: none"> <li>- The device interworks ISDN Setup with an Off Hook Indicator of "Voice" to SIP INVITE with "tgrp=hotline;trunk-context=dsn.mil" in the Contact header.</li> <li>- The device interworks ISDN Setup with an Off Hook indicator of "Data" to SIP INVITE with "tgrp=hotline-ccdata;trunk-context=dsn.mil" in the Contact header.</li> <li>- If ISDN Setup does not contain an Off Hook Indicator IE and the Bearer Capability IE contains "Unrestricted 64k", the outgoing INVITE includes "tgrp=ccdata;trunk-context=dsn.mil". If the Bearer Capability IE contains "Speech", the INVITE in this case does not contain tgrp and trunk-context parameters.</li> </ul> </li> <li><b>[4] Hotline Extended</b> = Interworks the ISDN Setup message's hotline "OffHook Indicator" Information Element (IE) to SIP INVITE's Request-URI and Contact headers. (Note: For IP-to-ISDN calls, the device handles the call as described in option <b>[3]</b>.) <ul style="list-style-type: none"> <li>✓ The device interworks ISDN Setup with an Off Hook Indicator of "Voice" to SIP INVITE Request-URI and Contact header with "tgrp=hotline;trunk-context=dsn.mil".</li> <li>✓ The device interworks ISDN Setup with an Off Hook indicator of "Data" to SIP INVITE Request-URI and Contact header with "tgrp=hotline-ccdata;trunk-context=dsn.mil".</li> <li>✓ If ISDN Setup does not contain an Off Hook Indicator IE and the Bearer Capability IE contains "Unrestricted 64k", the outgoing INVITE Request-URI and Contact header includes "tgrp=ccdata;trunk-context=dsn.mil". If the Bearer Capability IE contains "Speech", the INVITE in this case does not contain tgrp and trunk-context parameters.</li> </ul> </li> </ul> <p><b>Note:</b> IP-to-Tel configuration (using the PSTNPrefix parameter) overrides the 'tgrp' parameter in incoming INVITE messages.</p>
Web/EMS: TGRP Routing Precedence CLI: tgrp-routing-prec <b>[TGRPoutingPrecedence]</b>	<p>Determines the precedence method for routing IP-to-Tel calls - according to the Inbound IP Routing Table or according to the SIP 'tgrp' parameter.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) IP-to-Tel routing is determined by the Inbound IP Routing Table (PSTNPrefix parameter). If a matching rule is not found in this table, the device uses the Trunk Group parameters for</li> </ul>



Parameter	Description
	<p>routing the call.</p> <ul style="list-style-type: none"> <li>▪ <b>[1]</b> = The device first places precedence on the 'tgrp' parameter for IP-to-Tel routing. If the received INVITE Request-URI does not contain the 'tgrp' parameter or if the Trunk Group number is not defined, then the Inbound IP Routing Table is used for routing the call.</li> </ul> <p>Below is an example of an INVITE Request-URI with the 'tgrp' parameter, indicating that the IP call should be routed to Trunk Group 7:</p> <pre>INVITE sip:200;tgrp=7;trunk-context=example.com@10.33.2.68;user=phone SIP/2.0</pre> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For enabling routing based on the 'tgrp' parameter, the UseSIPTgrp parameter must be set to 2.</li> <li>▪ For IP-to-Tel routing based on the 'dtg' parameter (instead of the 'tgrp' parameter), use the parameter UseBroadsoftDTG.</li> </ul>
CLI: use-dtg <b>[UseBroadsoftDTG]</b>	<p>Determines whether the device uses the 'dtg' parameter for routing IP-to-Tel calls to a specific Trunk Group.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>When this parameter is enabled, if the Request-URI in the received SIP INVITE includes the 'dtg' parameter, the device routes the call to the Trunk Group according to its value. This parameter is used instead of the 'tgrp/trunk-context' parameters. The 'dtg' parameter appears in the INVITE Request-URI (and in the To header).</p> <p>For example, the received SIP message below routes the call to Trunk Group ID 56:</p> <pre>INVITE sip:123456@192.168.1.2;dtg=56;user=phone SIP/2.0</pre> <p><b>Note:</b> If the Trunk Group is not found based on the 'dtg' parameter, the Inbound IP Routing Table is used instead for routing the call to the appropriate Trunk Group.</p>
Web/EMS: Enable GRUU CLI: enable-gruu <b>[EnableGRUU]</b>	<p>Determines whether the Globally Routable User Agent URIs (GRUU) mechanism is used, according to RFC 5627. This is used for obtaining a GRUU from a registrar and for communicating a GRUU to a peer within a dialog.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>A GRUU is a SIP URI that routes to an instance-specific UA and can be reachable from anywhere. There are a number of contexts in which it is desirable to have an identifier that addresses a single UA (using GRUU) rather than the group of UA's indicated by an Address of Record (AOR). For example, in call transfer where user A is talking to user B, and user A wants to transfer the call to user C. User A sends a REFER to user C:</p> <pre>REFER sip:C@domain.com SIP/2.0 From: sip:A@domain.com;tag=99asd To: sip:C@domain.com Refer-To: (URI that identifies B's UA)</pre> <p>The Refer-To header needs to contain a URI that user C can use to place a call to user B. This call needs to route to the specific UA instance that user B is using to talk to user A. User B should provide user A with a URI that has to be usable by anyone. It needs to be a</p>

Parameter	Description
	<p>GRUU.</p> <ul style="list-style-type: none"> <li>Obtaining a GRUU: The mechanism for obtaining a GRUU is through registrations. A UA can obtain a GRUU by generating a REGISTER request containing a Supported header field with the value "gruu". The UA includes a "+sip.instance" Contact header parameter of each contact for which the GRUU is desired. This Contact parameter contains a globally unique ID that identifies the UA instance. The global unique ID is created from one of the following: <ul style="list-style-type: none"> <li>✓ If the REGISTER is per the device's client (endpoint), it is the MAC address concatenated with the phone number of the client.</li> <li>✓ If the REGISTER is per device, it is the MAC address only.</li> <li>✓ When using TP, "User Info" can be used for registering per endpoint. Thus, each endpoint can get a unique id – its phone number. The globally unique ID in TP is the MAC address concatenated with the phone number of the endpoint.</li> </ul> </li> </ul> <p>If the remote server doesn't support GRUU, it ignores the parameters of the GRUU. Otherwise, if the remote side also supports GRUU, the REGISTER responses contain the "gruu" parameter in each Contact header. This parameter contains a SIP or SIPS URI that represents a GRUU corresponding to the UA instance that registered the contact. The server provides the same GRUU for the same AOR and instance-id when sending REGISTER again after registration expiration. RFC 5627 specifies that the remote target is a GRUU target if its' Contact URL has the "gr" parameter with or without a value.</p> <ul style="list-style-type: none"> <li>Using GRUU: The UA can place the GRUU in any header field that can contain a URI. It must use the GRUU in the following messages: INVITE request, its 2xx response, SUBSCRIBE request, its 2xx response, NOTIFY request, REFER request and its 2xx response.</li> </ul>
EMS: Is CISCO Sce Mode [IsCiscoSCEMode]	<p>Determines whether a Cisco gateway exists at the remote side.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) No Cisco gateway exists at the remote side.</li> <li><b>[1]</b> = A Cisco gateway exists at the remote side.</li> </ul> <p>When a Cisco gateway exists at the remote side, the device must set the value of the 'annexb' parameter of the 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><b>Note:</b> The IsCiscoSCEMode parameter is applicable only when the selected coder is G.729.</p>
Web: User-Agent Information EMS: User Agent Display Info CLI: user-agent-info [UserAgentDisplayInfo]	<p>Defines the string that is used in the SIP User-Agent and Server response headers. When configured, the string &lt;UserAgentDisplayInfo value&gt;/software version' is used, for example:</p> <pre>User-Agent: myproduct/v.6.40.010.006</pre> <p>If not configured, the default string, &lt;AudioCodes product-name&gt;/software version' is used, for example:</p> <pre>User-Agent: Audiocodes-Sip-Gateway-Mediant 800 MSBR/v.6.40.010.006</pre> <p>The maximum string length is 50 characters.</p> <p><b>Note:</b> The software version number and preceding forward slash (/) cannot be modified. Therefore, it is recommended not to include a forward slash in the parameter's value (to avoid two forward slashes in the SIP header, which may cause problems).</p>
Web/EMS: SDP Session Owner	<p>Defines the value of the Owner line ('o' field) in outgoing SDP</p>



Parameter	Description
CLI: sdp-session-owner <b>[SIPSDPSessionOwner]</b>	<p>messages.</p> <p>The valid range is a string of up to 39 characters. The default is 'AudiocodesGW'.</p> <p>For example:</p> <pre>o=AudiocodesGW 1145023829 1145023705 IN IP4 10.33.4.126</pre>
CLI: sdp-ver-nego <b>[EnableSDPVersionNegotiation]</b>	<p>Enables the device to ignore new SDP re-offers (from the media negotiation perspective) in certain scenarios (such as session expires). According to RFC 3264, once an SDP session is established, a new SDP offer is considered a new offer only when the SDP origin value is incremented. In scenarios such as session expires, SDP negotiation is irrelevant and thus, the origin field is not changed.</p> <p>Even though some SIP devices don't follow this behavior and don't increment the origin value even in scenarios where they want to re-negotiate, the device can assume that the remote party operates according to RFC 3264, and in cases where the origin field is not incremented, the device does not re-negotiate SDP capabilities.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) The device negotiates any new SDP re-offer, regardless of the origin field.</li> <li>▪ <b>[1]</b> Enable = The device negotiates only an SDP re-offer with an incremented origin field.</li> </ul>
Web/EMS: Subject CLI: usr-def-subject <b>[SIPSubject]</b>	<p>Defines the Subject header value in outgoing INVITE messages. If not specified, the Subject header isn't included (default). The maximum length is up to 50 characters.</p>
<b>[CoderPriorityNegotiation]</b>	<p>Defines the priority for coder negotiation in the incoming SDP offer, between the device's or remote UA's coder list.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Coder negotiation is given higher priority to the remote UA's list of supported coders.</li> <li>▪ <b>[1]</b> = Coder negotiation is given higher priority to the device's (local) supported coders list.</li> <li>▪ Note: This parameter is applicable only to the Gateway/IP-to-IP application.</li> </ul>
Web: Send All Coders on Retrieve CLI: send-all-cdrs-on-rtrv <b>[SendAllCodersOnRetrieve]</b>	<p>Enables coder re-negotiation in the sent re-INVITE for retrieving an on-hold call.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) Sends only the initially chosen coder when the call was first established and then put on-hold.</li> <li>▪ <b>[1]</b> Enable = Includes all supported coders in the SDP of the re-INVITE sent to the call made un-hold (retrieved). The used coder is therefore, re-negotiated.</li> </ul> <p>This parameter is useful in the following call scenario example:</p> <ol style="list-style-type: none"> <li>1 Party A calls party B and coder G.711 is chosen.</li> <li>2 Party B is put on-hold while Party A blind transfers Party B to Party C.</li> <li>3 Party C answers and Party B is made un-hold. However, as Party C supports only G.729 coder, re-negotiation of the supported coder is required.</li> </ol> <p><b>Note:</b> This parameter is applicable only to the Gateway/IP-to-IP application.</p>

Parameter	Description
Web: Multiple Packetization Time Format EMS: Multi Ptime Format CLI: multi-ptime-format <b>[MultiPtimeFormat]</b>	<p>Determines whether the 'mptime' attribute is included in the outgoing SDP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> None = (Default) Disabled.</li> <li><b>[1]</b> PacketCable = Includes the 'mptime' attribute in the outgoing SDP - PacketCable-defined format.</li> </ul> <p>The 'mptime' attribute enables the device to define a separate packetization period for each negotiated coder in the SDP. The 'mptime' attribute is only included if this parameter is enabled even if the remote side includes it in the SDP offer. Upon receipt, each coder receives its 'ptime' value in the following precedence: from 'mptime' attribute, from 'ptime' attribute, and then from default value.</p>
EMS: Enable P Time <b>[EnablePtime]</b>	<p>Determines whether the 'ptime' attribute is included in the SDP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Remove the 'ptime' attribute from SDP.</li> <li><b>[1]</b> = (Default) Include the 'ptime' attribute in SDP.</li> </ul>
Web/EMS: 3xx Behavior CLI: 3xx-behavior <b>[3xxBehavior]</b>	<p>Determines the device's behavior regarding call identifiers when a 3xx response is received for an outgoing INVITE request. The device can either use the same call identifiers (Call-ID, To, and From tags) or change them in the new initiated INVITE.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Forward = (Default) Use different call identifiers for a redirected INVITE message.</li> <li><b>[1]</b> Redirect = Use the same call identifiers.</li> </ul>
Web/EMS: Enable P-Charging Vector CLI: p-charging-vector <b>[EnablePChargingVector]</b>	<p>Enables the inclusion of the P-Charging-Vector header to all outgoing INVITE messages.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Web/EMS: Retry-After Time CLI: retry-aftr-time <b>[RetryAfterTime]</b>	<p>Defines the time (in seconds) used in the Retry-After header when a 503 (Service Unavailable) response is generated by the device.</p> <p>The time range is 0 to 3,600. The default is 0.</p>
Web/EMS: Fake Retry After [sec] CLI: fake-retry-after <b>[FakeRetryAfter]</b>	<p>Determines whether the device, upon receipt of a SIP 503 response without a Retry-After header, behaves as if the 503 response included a Retry-After header and with the period (in seconds) specified by this parameter.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li>Any positive value (in seconds) for defining the period</li> </ul> <p>When enabled, this feature allows the device to operate with Proxy servers that do not include the Retry-After SIP header in SIP 503 (Service Unavailable) responses to indicate an unavailable service.</p> <p>The Retry-After header is used with the 503 (Service Unavailable) response to indicate how long the service is expected to be unavailable to the requesting SIP client. The device maintains a list of available proxies, by using the Keep-Alive mechanism. The device checks the availability of proxies by sending SIP OPTIONS every keep-alive timeout to all proxies.</p> <p>If the device receives a SIP 503 response to an INVITE, it also marks that the proxy is out of service for the defined "Retry-After" period.</p>
Web/EMS: Enable P-Associated-URI Header CLI: p-associated-uri-hdr <b>[EnablePAssociatedURI]</b>	<p>Determines the device usage of the P-Associated-URI header. This header can be received in 200 OK responses to REGISTER requests. When enabled, the first URI in the P-Associated-URI header is used in subsequent requests as the From/P-Asserted-Identity headers value.</p>

Parameter	Description
<b>Header]</b>	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> P-Associated-URIs in registration responses is handled only if the device is registered per endpoint (using the User Information file).</p>
Web/EMS: Source Number Preference CLI: src-nb-preference <b>[SourceNumberPreference]</b>	<p>Determines from which SIP header the source (calling) number is obtained in incoming INVITE messages.</p> <ul style="list-style-type: none"> <li>▪ If not configured (i.e., empty string) or if any string other than "From" or "Pai2" is configured, the calling number is obtained from a specific header using the following logic: <ul style="list-style-type: none"> <li>a. P-Preferred-Identity header.</li> <li>b. If the above header is not present, then the first P-Asserted-Identity header is used.</li> <li>c. If the above header is not present, then the Remote-Party-ID header is used.</li> <li>d. If the above header is not present, then the From header is used.</li> </ul> </li> <li>▪ <b>"From"</b> = The calling number is obtained from the From header.</li> <li>▪ <b>"Pai2"</b> = The calling number is obtained using the following logic: <ul style="list-style-type: none"> <li>a. If a P-Preferred-Identity header is present, the number is obtained from it.</li> <li>b. If no P-Preferred-Identity header is present and two P-Asserted-Identity headers are present, the number is obtained from the second P-Asserted-Identity header.</li> <li>c. If only one P-Asserted-Identity header is present, the calling number is obtained from it.</li> </ul> </li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The "From" and "Pai2" values are not case-sensitive.</li> <li>▪ Once a URL is selected, all the calling party parameters are set from this header. If P-Asserted-Identity is selected and the Privacy header is set to 'id', the calling number is assumed restricted.</li> </ul>
CLI: src-hdr-4-called-nb <b>[SelectSourceHeaderForCalledNumber]</b>	<p>Determines the SIP header used for obtaining the called number (destination) for IP-to-Tel calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Request-URI header = (Default) Obtains the destination number from the user part of the Request-URI.</li> <li>▪ <b>[1]</b> To header = Obtains the destination number from the user part of the To header.</li> <li>▪ <b>[2]</b> P-Called-Party-ID header = Obtains the destination number from the P-Called-Party-ID header.</li> </ul>
Web/EMS: Forking Handling Mode CLI: forking-handling <b>[ForkingHandlingMode]</b>	<p>Determines how the device handles the receipt of multiple SIP 18x forking responses for Tel-to-IP calls. The forking 18x response is the response with a different SIP to-tag than the previous 18x response. These responses are typically generated (initiated) by Proxy / Application servers that perform call forking, sending the device's originating INVITE (received from SIP clients) to several destinations, using the same CallID.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Parallel handling = (Default) If SIP 18x with SDP is received, the device opens a voice stream according to the received SDP and disregards any subsequently received 18x forking responses (with or without SDP). If the first response is 180 without SDP, the device responds according to the PlayRBTone2TEL parameter and disregards the subsequent forking 18x responses.</li> <li>▪ <b>[1]</b> Sequential handling = If 18x with SDP is received, the device</li> </ul>

Parameter	Description
	<p>opens a voice stream according to the received SDP. The device re-opens the stream according to subsequently received 18x responses with SDP, or plays a ringback tone if 180 response without SDP is received. If the first received response is 180 without SDP, the device responds according to the PlayRBTone2TEL parameter and processes the subsequent 18x forking responses.</p> <p><b>Note:</b> Regardless of this parameter setting, once a SIP 200 OK response is received, the device uses the RTP information and re-opens the voice stream, if necessary.</p>
Web: Forking Timeout CLI: forking-timeout <b>[ForkingTimeout]</b>	<p>Defines the timeout (in seconds) that is started after the first SIP 2xx response has been received for a User Agent when a Proxy server performs call forking (Proxy server forwards the INVITE to multiple SIP User Agents). The device sends a SIP ACK and BYE in response to any additional SIP 2xx received from the Proxy within this timeout. Once this timeout elapses, the device ignores any subsequent SIP 2xx.</p> <p>The number of supported forking calls per channel is 20. In other words, for an INVITE message, the device can receive up to 20 forking responses from the Proxy server.</p> <p>The valid range is 0 to 30. The default is 30.</p>
Web: Tel2IP Call Forking Mode CLI: tel2ip-call-forking-mode <b>[Tel2IPCallForkingMode]</b>	<p>Enables Tel-to-IP call forking, whereby a Tel call can be routed to multiple IP destinations.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> Once enabled, routing rules must be assigned Forking Groups in the Outbound IP Routing table.</p>
Web/EMS: Enable Reason Header CLI: reason-header <b>[EnableReasonHeader]</b>	<p>Enables the usage of the SIP Reason header.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable</li> <li>▪ <b>[1]</b> Enable (default)</li> </ul>
Web/EMS: Gateway Name CLI: gw-name <b>[SIPGatewayName]</b>	<p>Defines a name for the device (e.g., device123.com). This name is used as the host part of the SIP URI in the From header. If not specified, the device's IP address is used instead (default).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ Ensure that the parameter value is the one with which the Proxy has been configured with to identify the device.</li> <li>▪ This parameter can also be configured for an IP Group (in the IP Group table).</li> </ul>
<b>[ZeroSDPHandling]</b>	<p>Determines the device's response to an incoming SDP that includes an IP address of 0.0.0.0 in the SDP's Connection Information field (i.e., "c=IN IP4 0.0.0.0").</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Sets the IP address of the outgoing SDP's c= field to 0.0.0.0.</li> <li>▪ <b>[1]</b> = Sets the IP address of the outgoing SDP c= field to the IP address of the device. If the incoming SDP doesn't contain the "a=inactive" line, the returned SDP contains the "a=recvonly" line.</li> </ul>
Web/EMS: Enable Delayed Offer CLI: delayed-offer <b>[EnableDelayedOffer]</b>	<p>Determines whether the device sends the initial INVITE message with or without an SDP. Sending the first INVITE without SDP is typically done by clients for obtaining the far-end's full list of capabilities before sending their own offer. (An alternative method for obtaining the list of supported capabilities is by using SIP OPTIONS, which is not supported by every SIP agent.)</p>

Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) The device sends the initial INVITE message with an SDP.</li> <li>▪ <b>[1]</b> Enable = The device sends the initial INVITE message without an SDP.</li> </ul>
<b>[DisableCryptoLifeTimeSDP]</b>	<p>Enables the device to send "a=crypto" lines without the lifetime parameter in the SDP. For example, if the SDP contains "a=crypto:12 AES_CM_128_HMAC_SHA1_80 inline:hhQe10yZRcRcplFPkH5xYY9R1de37ogh9G1MpvNp 2^31", it removes the lifetime parameter "2^31".</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Web/EMS: Enable Contact Restriction CLI: contact-restriction <b>[EnableContactRestriction]</b>	<p>Determines whether the device sets the Contact header of outgoing INVITE requests to 'anonymous' for restricted calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
CLI: anonymous-mode <b>[AnonymousMode]</b>	<p>Determines whether the device's IP address is used as the URI host part instead of "anonymous.invalid" in the INVITE's From header for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) If the device receives a call from the Tel with blocked caller ID, it sends an INVITE with From: "anonymous"&lt;anonymous@anonymous.invalid&gt;</li> <li>▪ <b>[1]</b> = The device's IP address is used as the URI host part instead of "anonymous.invalid".</li> </ul> <p>This parameter may be useful, for example, for service providers who identify their SIP Trunking customers by their source phone number or IP address, reflected in the From header of the SIP INVITE. Therefore, even customers blocking their Caller ID can be identified by the service provider. Typically, if the device receives a call with blocked Caller ID from the PSTN side (e.g., Trunk connected to a PBX), it sends an INVITE to the IP with a From header as follows: From: "anonymous"&lt;anonymous@anonymous.invalid&gt;. This is in accordance with RFC 3325. However, when this parameter is set to 1, the device replaces the "anonymous.invalid" with its IP address.</p>
EMS: P Asserted User Name CLI: p-assrtd-usr-name <b>[PAssertedUserName]</b>	<p>Defines a 'representative number' (up to 50 characters) that is used as the user part of the Request-URI in the P-Asserted-Identity header of an outgoing INVITE for Tel-to-IP calls.</p> <p>The default value is null.</p>
EMS: Use URL In Refer To Header <b>[UseAORInReferToHeader]</b>	<p>Defines the source for the SIP URI set in the Refer-To header of outgoing REFER messages.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Use SIP URI from Contact header of the initial call.</li> <li>▪ <b>[1]</b> = Use SIP URI from To/From header of the initial call.</li> </ul>
Web: Enable User-Information Usage CLI: user-inf-usage <b>[EnableUserInfoUsage]</b>	<p>Enables the usage of the User Information, which is loaded to the device in the User Information auxiliary file. For a description on User Information, see 'Loading Auxiliary Files' on page 535.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[HandleReasonHeader]</b>	<p>Determines whether the device uses the value of the incoming SIP</p>

Parameter	Description
	Reason header for Release Reason mapping. <ul style="list-style-type: none"> <li><b>[0]</b> = Disregard Reason header in incoming SIP messages.</li> <li><b>[1]</b> = (Default) Use the Reason header value for Release Reason mapping.</li> </ul>
<b>[EnableSilenceSupplnSDP]</b>	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"> <li><b>[0]</b> = (Default) Disregard the 'silencesupp' attribute.</li> <li><b>[1]</b> = Handle incoming Re-INVITE messages that include the 'silencesupp:off' attribute in the SDP as a request to switch to the Voice-Band-Data (VBD) mode. In addition, the device includes the attribute 'a=silencesupp:off' in its SDP offer.</li> </ul> <p><b>Note:</b> This parameter is applicable only if the G.711 coder is used.</p>
<b>[EnableRport]</b>	Enables the usage of the 'rport' parameter in the Via header. <ul style="list-style-type: none"> <li><b>[0]</b> = Disabled (default)</li> <li><b>[1]</b> = Enabled</li> </ul> <p>The device adds an 'rport' parameter to the Via header of each outgoing SIP message. The first Proxy that receives this message sets the 'rport' value of the response to the actual port from where the request was received. This method is used, for example, to enable the device to identify its port mapping outside a NAT.</p> <p>If the Via header doesn't include the 'rport' parameter, the destination port of the response is obtained from the host part of the Via header.</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 destination port of the response is the port indicated in the 'rport' parameter.</p>
Web: Enable X-Channel Header EMS: X Channel Header CLI: x-channel-header <b>[XChannelHeader]</b>	Determines whether the SIP X-Channel header is added to SIP messages for providing information on the physical Trunk/B-channel on which the call is received or placed. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) X-Channel header is not used.</li> <li><b>[1]</b> Enable = X-Channel header is generated by the device and sent in INVITE messages and 180, 183, and 200 OK SIP responses. The header includes the Trunk number, B-channel, and the device's IP address.</li> </ul> <p>For example, 'x-channel: DS/DS1-5/8;IP=192.168.13.1', where:</p> <ul style="list-style-type: none"> <li>✓ 'DS/DS-1' is a constant string</li> <li>✓ '5' is the Trunk number</li> <li>✓ '8' is the B-channel</li> <li>✓ 'IP=192.168.13.1' is the device's IP address</li> </ul>
Web/EMS: Progress Indicator to IP CLI: prog-ind-2ip <b>[ProgressIndicator2IP]</b>	For Analog (FXS/FXO) interfaces: <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured = (Default) Default values are used. The default for FXO interfaces is 1; The default for FXS interfaces is 0.</li> <li><b>[0]</b> No PI = For IP-to-Tel calls, the device sends a 180 Ringing response to IP after placing a call to a phone (FXS) or PBX (FXO).</li> <li><b>[1]</b> PI = 1, <b>[8]</b> PI = 8: For IP-to-Tel calls, if the parameter EnableEarlyMedia is set to 1, the device sends a 183 Session Progress message with SDP immediately after a call is placed to a phone/PBX. This is used to cut-through the voice path before the remote party answers the call. This allows the originating party to listen to network Call Progress Tones (such as ringback tone or</li> </ul>



Parameter	Description
	<p>other network announcements).</p> <p>Digital interfaces:</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured = for ISDN spans, the progress indicator (PI) that is received in ISDN Proceeding, Progress, and Alerting messages is used as described in the options below. (default)</li> <li>▪ <b>[0]</b> No PI = For IP-to-Tel calls, the device sends 180 Ringing SIP response to IP after receiving ISDN Alerting or (for CAS) after placing a call to PBX/PSTN.</li> <li>▪ <b>[1]</b> PI =1, <b>[8]</b> PI =8: For IP-to-Tel calls, if the parameter EnableEarlyMedia is set to 1, the device sends 180 Ringing with SDP in response to an ISDN Alerting or it sends a 183 Session Progress message with SDP in response to only the first received ISDN Proceeding or Progress message after a call is placed to PBX/PSTN over the trunk.</li> </ul> <p><b>Note:</b> This parameter can also be configured per IP Profile (using the IPProfile parameter) and Tel Profile (using the TelProfile parameter).</p>
<b>[EnableRekeyAfter181]</b>	<p>Enables the device to send a re-INVITE with a new (different) SRTP key (in the SDP) if a SIP 181 response is received ("call is being forwarded"). The re-INVITE is sent immediately upon receipt of the 200 OK (when the call is answered).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul> <p><b>Note:</b> This parameter is applicable only if SRTP is used.</p>
<b>[NumberOfActiveDialogs]</b>	<p>Defines the maximum number of concurrent, outgoing SIP REGISTER dialogs. This parameter is used to control the registration rate. The valid range is 1 to 20. The default is 20.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ Once a 200 OK is received in response to a REGISTER message, the REGISTER message is not considered in this maximum count limit.</li> <li>▪ This parameter applies only to outgoing REGISTER messages (i.e., incoming is unlimited).</li> </ul>
EMS: Transparent Coder On Data Call <b>[TransparentCoderOnDataCall]</b>	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Only use coders from the coder list.</li> <li>▪ <b>[1]</b> = Use Transparent coder for data calls (according to RFC 4040).</li> </ul> <p>The Transparent coder can be used on data calls. When the device receives a Setup message from the ISDN with 'TransferCapabilities = data', it can initiate a call using the coder 'Transparent' (even if the coder is not included in the coder list).</p> <p>The initiated INVITE includes the following SDP attribute:</p> <pre>a=rtpmap:97 CLEARMODE/8000</pre> <p>The default payload type is set according to the CodersGroup parameter. If the Transparent coder is not defined, the default value is set to 56. The payload type is negotiated with the remote side, i.e., the selected payload type is according to the remote side selection. The receiving device must include the 'Transparent' coder in its coder list.</p>
Web: IP to IP Application CLI: enable-ip2ip <b>[EnableIP2IPApplication]</b>	<p>Enables the IP-to-IP Call Routing application.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>

Parameter	Description
<b>[IP2IPTranscodingMode]</b>	<p><b>Note:</b> This parameter is no longer valid and must not be used.</p> <p>Defines the voice transcoding mode (media negotiation) between two user agents for the IP-to-IP application. This parameter must always be set to 1 when using the IP-to-IP application.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Only if Required = Do not force transcoding. Many of the media settings (such as gain control) are not implemented on the voice stream. The device passes packets RTP to RTP packets without any processing.</li> <li><b>[1]</b> Force = (Default) Force transcoding on the outgoing IP leg. The device interworks the media by implementing DSP transcoding.</li> </ul>
Web: Enable RFC 4117 Transcoding CLI: rfc4117-trnsc-enbl <b>[EnableRFC4117Transcoding]</b>	<p>Enables transcoding of calls according to RFC 4117.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For more information on transcoding, see Transcoding using Third-Party Call Control on page <a href="#">519</a>.</li> </ul>
Web/EMS: Default Release Cause CLI: dflt-release-cse <b>[DefaultReleaseCause]</b>	<p>Defines the default Release Cause (sent to IP) for IP-to-Tel calls when the device initiates a call release and an explicit matching cause for this release is not found.</p> <p>The default release cause is NO_ROUTE_TO_DESTINATION (3). Other common values include NO_CIRCUIT_AVAILABLE (34), DESTINATION_OUT_OF_ORDER (27), etc.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The default release cause is described in the Q.931 notation and is translated to corresponding SIP 40x or 50x values (e.g., 3 to SIP 404, and 34 to SIP 503).</li> <li>Analog: For information on mapping PSTN release causes to SIP responses, see Mapping PSTN Release Cause to SIP Response on page <a href="#">318</a>.</li> <li>When the Trunk is disconnected or is not synchronized, the internal cause is 27. This cause is mapped, by default, to SIP 502.</li> <li>For mapping SIP-to-Q.931 and Q.931-to-SIP release causes, see Configuring Release Cause Mapping on page <a href="#">313</a>.</li> <li>For a list of SIP responses-Q.931 release cause mapping, see 'Alternative Routing to Trunk upon Q.931 Call Release Cause Code' on page <a href="#">339</a>.</li> </ul>
Web: Enable Microsoft Extension CLI: microsoft-ext <b>[EnableMicrosoftExt]</b>	<p>Enables the modification of the called and calling number for numbers received with Microsoft's proprietary "ext=xxx" parameter in the SIP INVITE URI user part. Microsoft Office Communications Server sometimes uses this proprietary parameter to indicate the extension number of the called or calling party.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>For example, if a calling party makes a call to telephone number 622125519100 Ext. 104, the device receives the SIP INVITE (from Microsoft's application) with the URI user part as INVITE sip:622125519100;ext=104@10.1.1.10 (or INVITE tel:622125519100;ext=104). If the parameter EnableMicrosoftExt is enabled, the device modifies the called number by adding an "e" as the prefix, removing the "ext=" parameter, and adding the extension number as the suffix (e.g., <b>e622125519100104</b>). Once modified, the device can</p>



Parameter	Description
	then manipulate the number further, using the Number Manipulation tables to leave only the last 3 digits (for example) for sending to a PBX.
EMS: Use SIP URI For Diversion Header [UseSIPURIForDiversionHeader]	Defines the URI format in the SIP Diversion header. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = 'tel:' (default)</li> <li>▪ <b>[1]</b> = 'sip:'</li> </ul>
[TimeoutBetween100And18x]	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).
[EnableImmediateTrying]	Determines if and when the device sends a 100 Trying in response to an incoming INVITE request. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = 100 Trying response is sent upon receipt of a Proceeding message from the PSTN.</li> <li>▪ <b>[1]</b> = (Default) 100 Trying response is sent immediately upon receipt of INVITE request.</li> </ul>
[TransparentCoderRepresentation]	Determines the format of the Transparent coder representation in the SDP. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = clearmode (default)</li> <li>▪ <b>[1]</b> = X-CCD</li> </ul>
[IgnoreRemoteSDPMKI]	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"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
[TrunkStatusReportingMode]	Determines whether the device responds to SIP OPTIONS if all the trunks pertaining to Trunk Group #1 are down or busy. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable = If all the trunks pertaining to Trunk Group #1 are down or busy, the device does not respond to received SIP OPTIONS.</li> </ul>
Web: Comfort Noise Generation Negotiation EMS: Comfort Noise Generation CLI: com-noise-gen-nego [ComfortNoiseNegotiation]	Enables negotiation and usage of Comfort Noise (CN). <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable</li> <li>▪ <b>[1]</b> Enable (default)</li> </ul> <p>The use of CN is indicated by including a payload type for CN on the media description line of the SDP. The device can use CN with a codec whose RTP time stamp clock rate is 8,000 Hz (G.711/G.726). The static payload type 13 is used. The use of CN is negotiated between sides. Therefore, if the remote side doesn't support CN, it is not used. Regardless of the device's settings, it always attempts to adapt to the remote SIP UA's request for CNG, as described below.</p> <p>To determine CNG support, the device uses the ComfortNoiseNegotiation parameter and the codec's SCE (silence suppression setting) using the CodersGroup parameter.</p> <p>If the ComfortNoiseNegotiation parameter is enabled, then the following occurs:</p> <ul style="list-style-type: none"> <li>▪ If the device is the initiator, it sends a "CN" in the SDP only if the SCE of the codec is enabled. If the remote UA responds with a "CN" in the SDP, then CNG occurs; otherwise, CNG does not occur.</li> <li>▪ If the device is the receiver and the remote SIP UA does not send a</li> </ul>

Parameter	Description
	<p>"CN" in the SDP, then no CNG occurs. If the remote side sends a "CN", the device attempts to be compatible with the remote side and even if the codec's SCE is disabled, CNG occurs.</p> <p>If the ComfortNoiseNegotiation parameter is disabled, then the device does not send "CN" in the SDP. However, if the codec's SCE is enabled, then CNG occurs.</p>
CLI: sdp-ecan-frmt <b>[SDPEcanFormat]</b>	<p>Defines the echo canceller format in the outgoing SDP. The 'ecan' attribute is used in the SDP to indicate the use of echo cancellation.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) The 'ecan' attribute appears on the 'a=gpmr' line.</li> <li><b>[1]</b> = The 'ecan' attribute appears as a separate attribute.</li> <li><b>[2]</b> = The 'ecan' attribute is not included in the SDP.</li> <li><b>[3]</b> = The 'ecan' attribute and the 'vbd' parameter are not included in the SDP.</li> </ul> <p><b>Note:</b> This parameter is applicable only when the IsFaxUsed parameter is set to 2, and for re-INVITE messages generated by the device as result of modem or fax tone detection.</p>
Web/EMS: First Call Ringback Tone ID CLI: 1st-call-rbt-id <b>[FirstCallIRBTId]</b>	<p>Defines the index of the first ringback tone in the CPT file. This option enables an Application server to request the device to play a distinctive ringback tone to the calling party according to the destination of the call. The tone is played according to the Alert-Info header received in the 180 Ringing SIP response (the value of the Alert-Info header is added to the value of this parameter).</p> <p>The valid range is -1 to 1,000. The default is -1 (i.e., play standard ringback tone).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>It is assumed that all ringback tones are defined in sequence in the CPT file.</li> <li>In case of an MLPP call, the device uses the value of this parameter plus 1 as the index of the ringback tone in the CPT file (e.g., if this value is set to 1, then the index is 2, i.e., 1 + 1).</li> </ul>
Web: Reanswer Time EMS: Regret Time CLI: reanswer-time <b>[RegretTime]</b>	<p>Analog: Defines the time interval from when the user hangs up the phone until the call is disconnected (FXS). This allows the user to hang up and then pick up the phone (before this timeout) to continue the call conversation. Thus, it's also referred to as regret time.</p> <p>Digital: Defines the time period the device waits for an MFC R2 Resume (Reanswer) signal once a Suspend (Clear back) signal is received from the PBX. If this timer expires, the call is released. Note that this is applicable only to the MFC-R2 CAS Brazil variant.</p> <p>The valid range is 0 to 255 (in seconds). The default is 0.</p>
Web: Enable Reanswering Info CLI: reans-info-enbl <b>[EnableReansweringINFO]</b>	<p>Enables the device to send a SIP INFO message with the On-Hook/Off-Hook parameter when the FXS phone goes on-hook during an ongoing call and then off-hook again, within the user-defined regret timeout (configured by the parameter RegretTime). Therefore, the device notifies the far-end that the call has been re-answered.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>This parameter is typically implemented for incoming IP-to-Tel collect calls to the FXS port. If the FXS user does not wish to accept the collect call, the user disconnects the call by on-hooking the phone. The device notifies the softswitch (or Application server) of the unanswered collect call (on-hook) by sending a SIP INFO message. As a result, the softswitch disconnects the call (sends a BYE message to the device). If</p>

Parameter	Description
	<p>the call is a regular incoming call and the FXS user on-hooks the phone without intending to disconnect the call, the softswitch does not disconnect the call (during the regret time).</p> <p>The INFO message format is as follows:</p> <pre>INFO sip:12345@10.50.228.164:5082 SIP/2.0 Via: SIP/2.0/UDP 127.0.0.1;branch=z9hG4bK_05_905924040-90579 From: &lt;sip:+551137077803@ims.acme.com.br:5080;user=phone&gt;;tag=008277765 To: &lt;sip:notavailable@unknown.invalid&gt;;tag=svw-0-1229428367 Call-ID: ConorCCR-0-LU-1229417827103300@dtas-stdn.fs5000group0-000.l CSeq: 1 INFO Contact: sip:10.20.7.70:5060 Content-Type: application/On-Hook (application/Off-Hook) Content-Length: 0</pre> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only if the parameter RegretTime is configured.</li> <li>▪ This parameter is applicable only to FXS interfaces.</li> </ul>
Web: PSTN Alert Timeout EMS: Trunk PSTN Alert Timeout CLI: pstn-alert-timeout <b>[PSTNAlertTimeout]</b>	<p>Digital: Defines the Alert Timeout (in seconds) for calls sent to the PSTN. This timer is used between the time a Setup message is sent to the Tel side (IP-to-Tel call establishment) and a Connect message is received. If an Alerting message is received, the timer is restarted. If the timer expires before the call is answered, the device disconnects the call and sends a SIP 408 request timeout response to the SIP party that initiated the call.</p> <p>Analog: Defines the Alert Timeout (in seconds) for calls to the Tel side. This timer is used between the time a ring is generated (FXS) or a line is seized (FXO), until the call is connected. For example: If the FXS device receives an INVITE, it generates a ring to the phone and sends a SIP 180 Ringing response to the IP. If the phone is not answered within the time interval set by this parameter, the device cancels the call by sending a SIP 408 response.</p> <p>The valid value range is 1 to 600 (in seconds). The default is 180.</p> <p><b>Note:</b> If per trunk configuration (using TrunkPSTNAlertTimeout) is set to other than default, the PSTNAlertTimeout parameter value is overridden.</p>
Web/EMS: RTP Only Mode CLI: rtp-only-mode <b>[RTPOnlyMode]</b>	<p>Enables the device to send and receive RTP packets to and from remote endpoints without the need to establish a SIP session. The remote IP address is determined according to the Outbound IP Routing table (Prefix parameter). The port is the same port as the local RTP port (configured by the BaseUDPPort parameter and the channel on which the call is received).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Transmit &amp; Receive = Send and receive RTP packets.</li> <li>▪ <b>[2]</b> Transmit Only= Send RTP packets only.</li> <li>▪ <b>[3]</b> Receive Only= Receive RTP packets only.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To activate the RTP Only feature without using ISDN / CAS signaling, you must do the following: <ul style="list-style-type: none"> <li>✓ Configure E1/T1 Transparent protocol type (set the ProtocoType</li> </ul> </li> </ul>

Parameter	Description
	<p>parameter to 5 or 6).</p> <ul style="list-style-type: none"> <li>✓ Enable the TDM-over-IP feature (set the EnableTDMoverIP parameter to 1).</li> <li>▪ To configure the RTP Only mode per trunk, use the RTPOnlyModeForTrunk_x parameter.</li> <li>▪ If per trunk configuration (using the RTPOnlyModeForTrunk_x parameter) is set to a value other than the default, the RTPOnlyMode parameter value is ignored.</li> </ul>
[RTPOnlyModeForTrunk_x]	<p>Enables the RTP Only feature per trunk, where ID denotes the trunk number (0 is the first trunk). For more information, see the RTPOnlyMode parameter.</p> <p><b>Note:</b> For using the global parameter (i.e., setting the RTP Only feature for all trunks), set this parameter to -1 (default).</p>
Web/EMS: SIT Q850 Cause [SITQ850Cause]	<p>Defines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when a Special Information Tone (SIT) is detected on an IP-to-Tel call.</p> <p>The valid range is 0 to 127. The default is 34.</p> <p><b>Note:</b> For mapping specific SIT tones, you can use the SITQ850CauseForNC, SITQ850CauseForIC, SITQ850CauseForVC, and SITQ850CauseForRO parameters.</p>
Web/EMS: SIT Q850 Cause For NC [SITQ850CauseForNC]	<p>Defines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-NC (No Circuit Found Special Information Tone) is detected from the TelPSTN for IP-to-Tel calls.</p> <p>The valid range is 0 to 127. The default is 34.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ When not configured (i.e., default), the SITQ850Cause parameter is used.</li> <li>▪ This parameter is applicable only to FXO interfaces.</li> </ul>
Web/EMS: SIT Q850 Cause For IC [SITQ850CauseForIC]	<p>Defines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-IC (Operator Intercept Special Information Tone) is detected from the PSTN for IP-to-Tel calls.</p> <p>The valid range is 0 to 127. The default is -1 (not configured).</p> <p><b>Note:</b> When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
Web/EMS: SIT Q850 Cause For VC [SITQ850CauseForVC]	<p>Defines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-VC (Vacant Circuit - non-registered number Special Information Tone) is detected from the PSTN for IP-to-Tel calls.</p> <p>The valid range is 0 to 127. The default is -1 (not configured).</p> <p><b>Note:</b> When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
Web/EMS: SIT Q850 Cause For RO [SITQ850CauseForRO]	<p>Defines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-RO (Reorder - System Busy Special Information Tone) is detected from the PSTN for IP-to-Tel calls.</p> <p>The valid range is 0 to 127. The default is -1 (not configured).</p> <p><b>Note:</b> When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
[GWInboundManipulationSet]	<p>Selects the Manipulation Set ID for manipulating all inbound INVITE messages. The Manipulation Set is defined using the MessageManipulations parameter. By default, no manipulation is done</p>

Parameter	Description
	(i.e. Manipulation Set ID is set to -1). <b>Note:</b> This parameter is applicable only to the Gateway/IP-to-IP application.
<b>[GWOOutboundManipulationSet]</b>	Selects the Manipulation Set ID for manipulating all outbound INVITE messages. The Manipulation Set is defined using the MessageManipulations parameter. By default, no manipulation is done (i.e. Manipulation Set ID is set to -1). <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is used only if the Outbound Message Manipulation Set parameter of the destination IP Group is not set.</li> <li>This parameter is applicable only to the Gateway/IP-to-IP application.</li> </ul>
<b>Out-of-Service (Busy Out) Parameters</b>	
Web/EMS: Enable Busy Out CLI: busy-out <b>[EnableBusyOut]</b>	<p>Enables the Busy Out feature.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (Default)</li> <li><b>[1]</b> Enable</li> </ul> <p>When Busy Out is enabled and certain scenarios exist, the device does the following:</p> <p>Analog: The FXS port behaves according to the settings of the FXSOOSBehavior parameter such as playing a reorder tone when the phone is off-hooked, or changing the line polarity.</p> <p>Digital: All E1/T1 trunks are automatically taken out of service by taking down the D-Channel or by sending a Service Out message for T1 PRI trunks supporting these messages (NI-2, 4/5-ESS, DMS-100, and Meridian).</p> <p>These behaviors are done upon one of the following scenarios:</p> <ul style="list-style-type: none"> <li>The device is physically disconnected from the network (i.e., Ethernet cable is disconnected).</li> <li>The Ethernet cable is connected, but the device is unable to communicate with any host. For this scenario, the LAN Watch-Dog must be activated (i.e., set the EnableLANWatchDog parameter to 1).</li> <li>The device can't communicate with the proxy (according to the Proxy Keep-Alive mechanism) and no other alternative route exists to send the call.</li> <li>The IP Connectivity mechanism is enabled (using the AltRoutingTel2IPEnable parameter) and there is no connectivity to any destination IP address.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Analog: The FXSOOSBehavior parameter determines the behavior of the FXS endpoints when a Busy Out or Graceful Lock occurs.</li> <li>Analog: FXO endpoints during Busy Out and Lock are inactive.</li> <li>Analog: See the LifeLineType parameter for complementary optional behavior.</li> <li>Digital: The Busy Out behavior depends on the PSTN protocol type.</li> <li>Digital: The Busy-Out condition can also be applied to a specific Trunk Group. If there is no connectivity to the Serving IP Group of a specific Trunk Group (defined in the Hunt Group Settings table), all physical trunks pertaining to that Trunk Group are set to the Busy-Out condition. Each trunk uses the proper Out-Of-Service method</li> </ul>

Parameter	Description
	<p>according to the selected ISDN/CAS variant.</p> <ul style="list-style-type: none"> <li>▪ Digital: To configure the method for setting digital trunks to Out-Of-Service, use the DigitalOOSBehavior parameter.</li> </ul>
Web/EMS: Graceful Busy Out Timeout [sec] CLI: graceful-busy-out-t-out <b>[GracefulBusyOutTimeout]</b>	<p>Defines the timeout interval (in seconds) for Out-of-Service graceful shutdown mode for busy trunks (per trunk) if communication fails with a Proxy server (or Proxy Set). In such a scenario, the device rejects new calls from the PSTN (Serving Trunk Group), but maintains currently active calls for this user-defined timeout. Once this timeout elapses, the device terminates currently active calls and takes the trunk out of service (sending the PSTN busy-out signal). Trunks on which no calls are active are immediately taken out of service regardless of the timeout.</p> <p>The range is 0 to 3,600. The default is 0.</p> <p><b>Note:</b> This parameter is applicable only to digital interfaces.</p>
Web: Digital Out-Of-Service Behavior EMS: Digital OOS Behavior For Trunk Value CLI: dig-oos-behavior <b>[DigitalOOSBehaviorForTrunk_x]</b>	<p>Determines the method for setting digital trunks to Out-of-Service state, per trunk.</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured = (Default) Use the settings of the DigitalOOSBehavior parameter for per device.</li> <li>▪ <b>[0]</b> Default = Uses default behavior for each trunk (see note below).</li> <li>▪ <b>[1]</b> Service = Sends ISDN In or Out of Service (only for ISDN protocols that support Service message).</li> <li>▪ <b>[2]</b> D-Channel = Takes D-Channel down or up (ISDN only).</li> <li>▪ <b>[3]</b> Alarm = Sends or clears PSTN AIS Alarm (ISDN and CAS).</li> <li>▪ <b>[4]</b> Block = Blocks trunk (CAS only).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only if the parameter EnableBusyOut is set to 1.</li> <li>▪ The default behavior (value 0) is as follows: <ul style="list-style-type: none"> <li>✓ <b>ISDN:</b> Use Service messages on supporting variants and use Alarm on non-supporting variants.</li> <li>✓ <b>CAS:</b> Use Alarm.</li> </ul> </li> <li>▪ When updating this parameter value at run-time, you must stop the trunk and then restart it for the update to take effect.</li> <li>▪ To determine the method for setting Out-Of-Service state for all trunks (i.e., per device), use the DigitalOOSBehavior parameter.</li> <li>▪ The x in the <i>ini</i> file parameter name denotes the trunk number, where 0 is the first trunk.</li> </ul>
Web: Digital Out-Of-Service Behavior CLI: dig-oos-behavior <b>[DigitalOOSBehavior]</b>	<p>Determines the method for setting digital trunks to Out-of-Service state. This configuration applies to all the device's trunks. For a description of this parameter's options, see the DigitalOOSBehaviorForTrunk_x parameter.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To configure the method for setting Out-of-Service state per trunk, use the DigitalOOSBehaviorForTrunk_x parameter.</li> <li>▪ To configure the timeout interval (in seconds) for Out-of-Service graceful shutdown mode for busy trunks if communication fails with a Proxy server (or Proxy Set), use the GracefulBusyOutTimeout parameter.</li> </ul>
Web: Out-Of-Service Behavior EMS: FXS OOS Behavior	<p>Determines the behavior of FXS endpoints when a Busy Out condition exists.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> None = Silence is heard when the FXS endpoint goes off-hook.</li> </ul>



Parameter	Description
CLI: oos-behavior <b>[FXSOOSBehavior]</b>	<ul style="list-style-type: none"> <li><b>[1]</b> Reorder Tone = (Default) The device plays a reorder tone to the connected phone / PBX.</li> <li><b>[2]</b> Polarity Reversal = The device reverses the polarity of the endpoint making it unusable (relevant, for example, for PBX DID lines).</li> <li><b>[3]</b> Reorder Tone + Polarity Reversal = Same as options [1] and [2].</li> <li><b>[4]</b> Current Disconnect = The device disconnects the current to the FXS endpoint.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>A device reset is required for this parameter to take effect when it is set to [2], [3], or [4].</li> <li>This parameter is applicable only to FXS interfaces.</li> </ul>
<b>Retransmission Parameters</b>	
Web: SIP T1 Retransmission Timer <b>[msec]</b> EMS: T1 RTX CLI: t1-re-tx-time <b>[SipT1Rtx]</b>	Defines the time interval (in msec) between the first transmission of a SIP message and the first retransmission of the same message. The default is 500. <p><b>Note:</b> The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx. For INVITE requests, it is multiplied by two for each new retransmitted message. For all other SIP messages, it is multiplied by two until SipT2Rtx. For example, assuming SipT1Rtx = 500 and SipT2Rtx = 4000:</p> <ul style="list-style-type: none"> <li>The first retransmission is sent after 500 msec.</li> <li>The second retransmission is sent after 1000 (2*500) msec.</li> <li>The third retransmission is sent after 2000 (2*1000) msec.</li> <li>The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec.</li> </ul>
Web: SIP T2 Retransmission Timer <b>[msec]</b> EMS: T2 RTX CLI: t2-re-tx-time <b>[SipT2Rtx]</b>	Defines the maximum interval (in msec) between retransmissions of SIP messages (except for INVITE requests). The default is 4000. <p><b>Note:</b> The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.</p>
Web: SIP Maximum RTX EMS: Max RTX CLI: sip-max-rtx <b>[SIPMaxRtx]</b>	Defines the maximum number of UDP transmissions of SIP messages (first transmission plus retransmissions). The range is 1 to 30. The default is 7.
Web: Number of RTX Before Hot-Swap EMS: Proxy Hot Swap Rtx CLI: nb-of-rtx-b4-hot-swap <b>[HotSwapRtx]</b>	Defines the number of retransmitted INVITE/REGISTER messages before the call is routed (hot swap) to another Proxy/Registrar. The valid range is 1 to 30. The default is 3. <p><b>Note:</b> This parameter is also used for alternative routing. If a domain name in the Outbound IP Routing Table or SBC IP-to-IP Routing table is resolved into two IP addresses, and if there is no response for HotSwapRtx retransmissions to the INVITE message that is sent to the first IP address, the device immediately initiates a call to the second IP address.</p>
<b>SIP Message Manipulations Table</b>	
Web: Message Manipulations EMS: Message	This table parameter defines manipulation rules for SIP header messages.

Parameter	Description
Manipulations CLI: configure voip > sbc manipulations message- manipulations <b>[MessageManipulations]</b>	The format of this parameter is as follows: <b>[ MessageManipulations]</b> FORMAT MessageManipulations_Index = MessageManipulations_ManSetID, MessageManipulations_MessageType, MessageManipulations_Condition, MessageManipulations_ActionSubject, MessageManipulations_ActionType, MessageManipulations_ActionValue, MessageManipulations_RowRole; <b>[MessageManipulations]</b> 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; <b>Note:</b> For a detailed description of this table, see 'Configuring SIP Message Manipulation' on page <a href="#">226</a> .
<b>Message Policy Table</b>	
Web: Message Policy Table CLI: configure voip > sbc message-policy <b>[MessagePolicy]</b>	This table parameter configures SIP message policy rules for blocking (blacklist) unwanted incoming SIP messages or allowing (whitelist) receipt of desired messages. The format of this parameter is as follows: <b>[MessagePolicy]</b> FORMAT MessagePolicy_Index = MessagePolicy_Policy, MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength, MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders, MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection, MessagePolicy_MethodListType, MessagePolicy_MethodList, MessagePolicy_BodyListType, MessagePolicy_BodyList; <b>[/MessagePolicy]</b> <b>Note:</b> For a detailed description of this table, see 'Configuring SIP Message Policy Rules'.

## 59.9 Coders and Profile Parameters

The profile parameters are described in the table below.

**Profile Parameters**

Parameter	Description
<b>Coders Table / Coder Groups Table</b>	
Web: Coders Table/Coder Group Settings EMS: Coders Group CLI: configure voip > coders-and-profiles coders-group <b>[CodersGroup0]</b> <b>[CodersGroup1]</b> <b>[CodersGroup2]</b> <b>[CodersGroup3]</b> <b>[CodersGroup4]</b>	This table parameter 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 this parameter is as follows: <b>[ CodersGroup&lt;0-9&gt; ]</b> FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime, CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce; <b>[ \CodersGroup&lt;0-9&gt; ]</b> For example, below are defined two Coder Groups (0 and 1):



Parameter	Description
<b>[CodersGroup5]</b> <b>[CodersGroup6]</b> <b>[CodersGroup7]</b> <b>[CodersGroup8]</b> <b>[CodersGroup9]</b>	<p><b>[ CodersGroup0 ]</b>            FORMAT CodersGroup0_Index = CodersGroup0_Name,            CodersGroup0_pTime, CodersGroup0_rate,            CodersGroup0_PayloadType, CodersGroup0_Sce;            CodersGroup0 0 = g711Alaw64k, 20, 0, 255, 0;            CodersGroup0 1 = eg711Ulaw, 10, 0, 71, 0;            CodersGroup0 2 = eg711Ulaw, 10, 0, 71, 0;  <b>[ \CodersGroup0 ]</b></p> <p><b>[ CodersGroup1 ]</b>            FORMAT CodersGroup1_Index = CodersGroup1_Name,            CodersGroup1_pTime, CodersGroup1_rate,            CodersGroup1_PayloadType, CodersGroup1_Sce;            CodersGroup1 0 = Transparent, 20, 0, 56, 0;            CodersGroup1 1 = g726, 20, 0, 23, 0;  <b>[ \CodersGroup1 ]</b></p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For a list of supported coders and a detailed description of this table, see Configuring Coders on page <a href="#">233</a>.</li> <li>The coder name is case-sensitive.</li> </ul>
<b>IP Profile Table</b>	
Web: IP Profile Settings EMS: Protocol Definition > IP Profile CLI: configure voip > coders-and-profiles ip- profile <b>[IPProfile]</b>	<p>This table parameter configures the IP Profile table. Each IP Profile ID includes a set of parameters (which are typically configured separately using their individual "global" parameters). You can later assign these IP Profiles to outbound IP routing rules (Prefix parameter), inbound IP routing rules and IP Groups.</p> <p>The format of this parameter is as follows:  <b>[IPProfile]</b>            FORMAT IpProfile_Index = IpProfile_ProfileName,            IpProfile_IpPreference, IpProfile_CodersGroupID, IpProfile_IsFaxUsed,            IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,            IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,            IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,            IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode,            IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP,            IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP,            IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber,            IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit,            IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption,            IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption,            IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume,            IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID,            IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,            IpProfile_SBCAllowedCodersGroupID,            IpProfile_SBCAllowedCodersMode,            IpProfile_SBCMediaSecurityBehaviour,            IpProfile_SBCRFC2833Behavior,            IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,            IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,            IpProfile_AMDMaxGreetingTime,            IpProfile_AMDMaxPostSilenceGreetingTime,            IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode,            IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,            IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode,            IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode,</p>

Parameter	Description
	<p>IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport, IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior, IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport, IpProfile_SBCRemoteEarlyMediaResponseType, IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI, IpProfile_MKISize, IpProfile_SBCEnforceMKISize, IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960, IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183, IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType, IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey, IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource, IpProfile_SBCPlayHeldTone, IpProfile_SBCRemoteHoldFormat, IpProfile_DelayTimeForInvite; [IPProfile]</p> <p><b>Note:</b> For a description of this table, see 'Configuring IP Profiles' on page 239.</p>
Tel Profile Table	
<p>Web: Tel Profile Settings EMS: Protocol Definition &gt; Telephony Profile CLI: configure voip &gt; coders-and-profiles tel-profile <b>[TelProfile]</b></p>	<p>This table parameter configures the Tel Profile table. Each Tel Profile ID includes a set of parameters (which are typically configured separately using their individual, "global" parameters). You can later assign these Tel Profile IDs to other elements such as in the Trunk Group TableEndpoint Phone Number table (TrunkGroup parameter). Therefore, Tel Profiles allow you to apply the same settings of a group of parameters to multiple channels, or apply specific settings to different channels.</p> <p>The format of this parameter is as follows:</p> <p><b>[TelProfile]</b>  FORMAT TelProfile_Index = TelProfile_ProfileName, TelProfile_TelPreference, TelProfile_CodersGroupID, TelProfile_IsFaxUsed, TelProfile_JitterBufMinDelay, TelProfile_JitterBufOptFactor, TelProfile_IPDiffServ, TelProfile_SigIPDiffServ, TelProfile_DtmfVolume, TelProfile_InputGain, TelProfile_VoiceVolume, TelProfile_EnableReversePolarity, TelProfile_EnableCurrentDisconnect, TelProfile_EnableDigitDelivery, TelProfile_EnableEC, TelProfile_MWIAAnalog, TelProfile_MWIDisplay, TelProfile_FlashHookPeriod, TelProfile_EnableEarlyMedia, TelProfile_ProgressIndicator2IP, TelProfile_TimeForReorderTone, TelProfile_EnableDIDWink, TelProfile_IsTwoStageDial, TelProfile_DisconnectOnBusyTone, TelProfile_EnableVoiceMailDelay, TelProfile_DialPlanIndex, TelProfile_Enable911PSAP, TelProfile_SwapTelToIPPhoneNumbers, TelProfile_EnableAGC, TelProfile_ECNIPMode, TelProfile_DigitalCutThrough, TelProfile_EnableFXODoubleAnswer, TelProfile_CallPriorityMode;  <b>[TelProfile]</b></p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For a description of this parameter, see Configuring Tel Profiles on page 237.</li> <li>For a detailed description of each parameter, see its corresponding "global" parameter.</li> </ul>

Parameter	Description		
	TelProfile Field	Web Name	Global Parameter
	TelProfile_ProfileName	Profile Name	-
	TelProfile_TelPreference	Profile Preference	-
	TelProfile_CodersGroupID	Coder Group	CodersGroup0
	TelProfile_IsFaxUsed	Fax Signaling Method	IsFaxUsed
	TelProfile_JitterBufMinDelay	Dynamic Jitter Buffer Minimum Delay	DJBufMinDelay
	TelProfile_JitterBufOptFactor	Dynamic Jitter Buffer Optimization Factor	DJBufOptFactor
	TelProfile_IPDiffServ	RTP IP DiffServ	PremiumServiceClassMediaDiffServ
	TelProfile_SigIPDiffServ	Signaling DiffServ	PremiumServiceClassControlDiffServ
	TelProfile_DtmfVolume	DTMF Volume	DTMFVolume
	TelProfile_InputGain	Input Gain	InputGain
	TelProfile_VoiceVolume	Voice Volume	VoiceVolume
	TelProfile_EnableReversePolarity	Enable Polarity Reversal	EnableReversalPolarity
	TelProfile_EnableCurrentDisconnect	Enable Current Disconnect	EnableCurrentDisconnect
	TelProfile_EnableDigitDelivery	Enable Digit Delivery	EnableDigitDelivery
	TelProfile_EnableEC	Echo Canceler	EnableEchoCanceller
	TelProfile_MWIAnalog	MWI Analog Lamp	MWIAnalogLamp
	TelProfile_MWIDisplay	MWI Display	MWIDisplay
	TelProfile_FlashHookPeriod	Flash Hook Period	FlashHookPeriod
	TelProfile_EnableEarlyMedia	Enable Early Media	EnableEarlyMedia
	TelProfile_ProgressIndicator2IP	Progress Indicator to IP	ProgressIndicator2IP
	TelProfile_TimeForReorderTone	Time For Reorder Tone	TimeForReorderTone
	TelProfile_EnabledIDWink	Enable DID Wink	EnableDIDWink
	TelProfile_IsTwoStageDial	Dialing Mode	IsTwoStageDial
	TelProfile_DisconnectOnBusyTone	Disconnect Call on Detection of Busy Tone	DisconnectOnBusyTone
	TelProfile_EnableVoiceMailDelay	Enable Voice Mail Delay	-
	TelProfile_DialPlanIndex	Dial Plan Index	DialPlanIndex
	TelProfile_Enable911PSAP	Enable 911 PSAP	Enable911PSAP
	TelProfile_SwapTelToIPPhoneNumbers	Swap Tel To IP Phone Numbers	SwapTEI2IPCalled&CallingNumbers

Parameter	Description			
	TelProfile_EnableAGC	Enable AGC	EnableAGC	
	TelProfile_ECNlpMode	EC NLP Mode	ECNLPMode	
	TelProfile_DigitalCutThrough	-	DigitalCutThrough	
	TelProfile_EnableFXODoubleAnswer	-	EnableFXODoubleAnswer	
	TelProfile_CallPriorityMode	-	CallPriorityMode	

## 59.10 Channel Parameters

This subsection describes the device's channel parameters.

### 59.10.1 Voice Parameters

The voice parameters are described in the table below.

**Voice Parameters**

Parameter	Description
Web/EMS: Input Gain CLI: input-gain <b>[InputGain]</b>	Defines the pulse-code modulation (PCM) input gain control (in decibels). This parameter sets the level for the received (Tel/PSTN-to-IP) signal. The valid range is -32 to 31 dB. The default is 0 dB. <b>Note:</b> This parameter can also be configured in an IP Profile and/or a Tel Profile.
Web: Voice Volume EMS: Volume (dB) CLI: voice-volume <b>[VoiceVolume]</b>	Defines the voice gain control (in decibels). This parameter sets the level for the transmitted (IP-to-Tel/PSTN) signal. The valid range is -32 to 31 dB. The default is 0 dB. <b>Note:</b> This parameter can also be configured in an IP Profile and/or a Tel Profile.
EMS: Payload Format CLI: G726-voice-payload-format <b>[VoicePayloadFormat]</b>	Determines the bit ordering of the G.726/G.727 voice payload format. <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Little Endian</li> <li><b>[1]</b> = Big Endian</li> </ul> <b>Note:</b> To ensure high voice quality when using G.726/G.727, both communicating ends should use the same endianness format. Therefore, when the device communicates with a third-party entity that uses the G.726/G.727 voice coder and voice quality is poor, change the settings of this parameter (between Big Endian and Little Endian).
Web: MF Transport Type CLI: MF-transport-type <b>[MFTransportType]</b>	Currently, not supported.
Web: Enable Answer Detector <b>[EnableAnswerDetector]</b>	Currently, not supported.
Web: Answer Detector Activity Delay	Defines the time (in 100-msec resolution) between activating the Answer Detector and the time that the detector actually starts to

Parameter	Description
CLI: answer-detector-activity-delay <b>[AnswerDetectorActivityDelay]</b>	operate. The valid range is 0 to 1023. The default is 0.
Web: Answer Detector Silence Time <b>[AnswerDetectorSilenceTime]</b>	Currently, not supported.
Web: Answer Detector Redirection <b>[AnswerDetectorRedirection]</b>	Currently, not supported.
Web: Answer Detector Sensitivity EMS: Sensitivity CLI: answer-detector-sensitivity <b>[AnswerDetectorSensitivity]</b>	Defines the Answer Detector sensitivity. The range is 0 (most sensitive) to 2 (least sensitive). The default is 0.
Web: Silence Suppression EMS: Silence Compression Mode CLI: silence-compression-mode <b>[EnableSilenceCompression]</b>	Determines the Silence Suppression support. Silence Suppression is a method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Silence Suppression is disabled.</li> <li><b>[1]</b> Enable = Silence Suppression is enabled.</li> <li><b>[2]</b> Enable without Adaptation = A single silence packet is sent during a silence period (applicable only to G.729).</li> </ul> <b>Note:</b> If the selected coder is G.729, the value of the 'annexb' parameter of the fmp attribute in the SDP is determined by the following rules: <ul style="list-style-type: none"> <li>If EnableSilenceCompression is 0: 'annexb=no'.</li> <li>If EnableSilenceCompression is 1: 'annexb=yes'.</li> <li>If EnableSilenceCompression is 2 and IsCiscoSCEMode is 0: 'annexb=yes'.</li> <li>If EnableSilenceCompression is 2 and IsCiscoSCEMode is 1: 'annexb=no'.</li> </ul>
Web: Echo Canceller EMS: Echo Canceller Enable CLI: echo-canceller-enable <b>[EnableEchoCanceller]</b>	Enables echo cancellation (i.e., echo from voice calls is removed). <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul> <b>Note:</b> This parameter can also be configured in an IP Profile and/or a Tel Profile.
Web: Network Echo Suppressor Enable CLI: acoustic-echo-suppressor-enable <b>[AcousticEchoSuppressorSupport]</b>	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"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: Echo Canceller Type CLI: echo-canceller-type <b>[EchoCancellerType]</b>	Defines the echo canceller type. <ul style="list-style-type: none"> <li><b>[0]</b> Line echo canceller = (Default) Echo canceller for Tel side.</li> <li><b>[1]</b> Acoustic Echo suppressor - netw = Echo canceller for IP side.</li> </ul>

Parameter	Description
Web: Attenuation Intensity CLI: acoustic-echo-suppressor-attenuation-intensity <b>[AcousticEchoSuppAttenuationIntensity]</b>	Defines the acoustic echo suppressor signals identified as echo attenuation intensity. The valid range is 0 to 3. The default is 0.
Web: Max ERL Threshold - DB CLI: acoustic-echo-suppressor-max-ERL <b>[AcousticEchoSuppMaxERLThreshold]</b>	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.
Web: Min Reference Delay x10 msec CLI: acoustic-echo-suppressor-min-reference-delay <b>[AcousticEchoSuppMinRefDelayx10ms]</b>	Defines the acoustic echo suppressor minimum reference delay (in 10-ms units). The valid range is 0 to 40. The default is 0.
Web: Max Reference Delay x10 msec CLI: acoustic-echo-suppressor-max-reference-delay <b>[AcousticEchoSuppMaxRefDelayx10ms]</b>	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).
EMS: Echo Canceller Hybrid Loss CLI: echo-canceller-hybrid-loss <b>[ECHybridLoss]</b>	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"> <li>▪ <b>[0]</b> = (Default) 6 dB</li> <li>▪ <b>[1]</b> = N/A</li> <li>▪ <b>[2]</b> = 0 dB</li> <li>▪ <b>[3]</b> = 3 dB</li> </ul>
EMS: ECN Ip Mode CLI: echo-canceller-NLP-mode <b>[ECNLPMode]</b>	Defines the echo cancellation Non-Linear Processing (NLP) mode. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) NLP adapts according to echo changes</li> <li>▪ <b>[1]</b> = Disables NLP</li> <li>▪ <b>[2]</b> = Silence output NLP</li> </ul> <b>Note:</b> This parameter can also be configured in a Tel Profile.
CLI: echo-canceller-aggressive-NLP <b>[EchoCancellerAggressiveNLP]</b>	Enables the Aggressive NLP at the first 0.5 second of the call. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable</li> <li>▪ <b>[1]</b> = (Default) Enable. The echo is removed only in the first half of a second of the incoming IP signal.</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
CLI: number-of-SID-coefficients <b>[RTPSIDCoeffNum]</b>	Defines the number of spectral coefficients added to an SID packet being sent according to RFC 3389. The valid values are <b>[0]</b> (default), <b>[4]</b> , <b>[6]</b> , <b>[8]</b> and <b>[10]</b> .

## 59.10.2 Coder Parameters

The coder parameters are described in the table below.

**Coder Parameters**

Parameter	Description
Silk Tx Inband FEC CLI: silk-tx-inband-fec <b>[SilkTxInbandFEC]</b>	Enables forward error correction (FEC) for the SILK coder. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Silk Max Average Bit Rate CLI: silk-max-average-bitrate <b>[SilkMaxAverageBitRate]</b>	Defines the maximum average bit rate for the SILK coder. The valid value range is 5000 to 30000. The default is 16000. <b>Note:</b> The SILK coder is Skype's default audio codec used for Skype-to-Skype calls.
CLI: EVRC-VAD-enable <b>[EnableEVRCVAD]</b>	Enables the EVRC voice activity detector. <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul> <b>Note:</b> Supported for EVRC and EVRC-B coders.
EMS: VBR Coder DTX Min CLI: EVRC-dtx-min <b>[EVRCDTXMin]</b>	Defines the minimum gap between two SID frames when using the EVRC voice activity detector. Units are in EVRC frame size (20 msec). The range is 0 to 20000. The default is 12. <b>Note:</b> Supported for EVRC and EVRC-B coders.
EMS: VBR Coder DTX Max CLI: EVRC-dtx-max <b>[EVRCDTXMax]</b>	Defines the maximum gap between two SID frames when using the EVRC voice activity detector. Units are in EVRC frame size (20 msec). The range is 0 to 20000. The default is 32. <b>Note:</b> This parameter is applicable only to EVRC and EVRC-B coders.
EMS: VBR Coder Header Format CLI: VBR-coder-header-format <b>[VBRCoderHeaderFormat]</b>	Determines the format of the RTP header for VBR coders. <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Payload only (no header, TOC, or m-factor) - similar to RFC 3558 Header Free format.</li> <li><b>[1]</b> = Supports RFC 2658 - 1 byte for interleaving header (always 0), TOC, no m-factor.</li> <li><b>[2]</b> = Payload including TOC only, allow m-factor.</li> <li><b>[3]</b> = RFC 3558 Interleave/Bundled format.</li> </ul>
EMS: VBR Coder Hangover CLI: VBR-coder-hangover <b>[VBRCoderHangover]</b>	Defines the required number of silence frames at the beginning of each silence period when using the VBR coder silence suppression. The range is 0 to 255. The default is 1.
Web: AMR Payload Format <b>[AmrOctetAlignedEnable]</b>	Defines the AMR payload format type. <ul style="list-style-type: none"> <li><b>[0]</b> Bandwidth Efficient</li> <li><b>[1]</b> Octet Aligned (default)</li> </ul>



### 59.10.3 DTMF Parameters

The dual-tone multi-frequency (DTMF) parameters are described in the table below.

**DTMF Parameters**

Parameter	Description
Web/EMS: DTMF Transport Type CLI: DTMF-transport-type <b>[DTMFTransportType]</b>	<p>Determines the DTMF transport type.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Mute DTMF = DTMF digits are removed from the voice stream and are not relayed to remote side.</li> <li>▪ <b>[2]</b> Transparent DTMF = DTMF digits remain in the voice stream.</li> <li>▪ <b>[3]</b> RFC 2833 Relay DTMF = (Default) DTMF digits are removed from the voice stream and are relayed to remote side according to RFC 2833.</li> <li>▪ <b>[7]</b> RFC 2833 Relay Decoder Mute = DTMF digits are sent according to RFC 2833 and muted when received.</li> </ul> <p><b>Note:</b> This parameter is automatically updated if the parameters TxDTMFOption or RxDTMFOption are configured.</p>
Web: DTMF Volume (-31 to 0 dB) EMS: DTMF Volume (dBm) CLI: DTMF-volume <b>[DTMFVolume]</b>	<p>Defines the DTMF gain control value (in decibels) to the PSTN or analog side.</p> <p>The valid range is -31 to 0 dB. The default is -11 dB.</p> <p><b>Note:</b> This parameter can also be configured in a Tel Profile.</p>
Web: DTMF Generation Twist EMS: DTMF Twist Control CLI: DTMF-generation-twist <b>[DTMFGenerationTwist]</b>	<p>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.</p> <p>The valid range is -10 to 10 dB. The default is 0 dB.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: DTMF Inter Interval (msec) CLI: inter-digit-interval <b>[DTMFInterDigitInterval]</b>	<p>Defines the time (in msec) between generated DTMF digits to PSTN side (if TxDTMFOption = 1, 2 or 3).</p> <p>The valid range is 0 to 32767. The default is 100 msec.</p>
EMS: DTMF Length (msec) <b>[DTMFDigitLength]</b>	<p>Defines the time (in msec) for generating DTMF tones to the PSTN side (if TxDTMFOption = 1, 2 or 3). It also configures the duration that is sent in INFO (Cisco) messages.</p> <p>The valid range is 0 to 32767. The default is 100.</p>
EMS: Rx DTMF Relay Hang Over Time (msec) CLI: default-dtmf-signal-duration <b>[RxDTMFHangOverTime]</b>	<p>Defines the Voice Silence time (in msec) after playing DTMF or MF digits to the Tel/PSTN side that arrive as Relay from the IP side.</p> <p>Valid range is 0 to 2,000 msec. The default is 1,000 msec.</p>
EMS: Tx DTMF Relay Hang Over Time (msec) CLI: digit-hangover-time-tx <b>[TxDTMFHangOverTime]</b>	<p>Defines the Voice Silence time (in msec) after detecting the end of DTMF or MF digits at the Tel/PSTN side when the DTMF Transport Type is either Relay or Mute.</p> <p>Valid range is 0 to 2,000 msec. The default is 1,000 msec.</p>
Web/EMS: NTE Max Duration CLI: telephony-events-max-duration	<p>Defines the maximum time for sending Named Telephony Events / NTEs (RFC 4733/2833 DTMF relay) to the IP side, regardless of</p>



Parameter	Description
<b>[NTEMaxDuration]</b>	the DTMF signal duration on the TDM 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).

### 59.10.4 RTP, RTCP and T.38 Parameters

The RTP, RTCP and T.38 parameters are described in the table below.

#### RTP/RTCP and T.38 Parameters

Parameter	Description
Web: Dynamic Jitter Buffer Minimum Delay EMS: Minimal Delay (dB) CLI: jitter-buffer-minimum-delay <b>[DJBufMinDelay]</b>	Defines the minimum delay (in msec) for the Dynamic Jitter Buffer. The valid range is 0 to 150. The default delay is 10. <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter can also be configured in an IP Profile and/or a Tel Profile.</li> <li>For more information on Jitter Buffer, see Dynamic Jitter Buffer Operation on page 161.</li> </ul>
Web: Dynamic Jitter Buffer Optimization Factor EMS: Opt Factor CLI: jitter-buffer-optimization-factor <b>[DJBufOptFactor]</b>	Defines the Dynamic Jitter Buffer frame error/delay optimization factor. The valid range is 0 to 12. The default factor is 10. <b>Notes:</b> <ul style="list-style-type: none"> <li>For data (fax and modem) calls, set this parameter to 12.</li> <li>This parameter can also be configured in an IP Profile and/or a Tel Profile.</li> <li>For more information on Jitter Buffer, see Dynamic Jitter Buffer Operation on page 161.</li> </ul>
Web/EMS: Analog Signal Transport Type <b>[AnalogSignalTransportType]</b>	Determines the analog signal transport type. <ul style="list-style-type: none"> <li><b>[0]</b> Ignore Analog Signals = (Default) Ignore.</li> <li><b>[1]</b> RFC 2833 Analog Signal Relay = Transfer hookflash using RFC 2833.</li> </ul>
Web: RTP Redundancy Depth EMS: Redundancy Depth CLI: RTP-redundancy-depth <b>[RTPRedundancyDepth]</b>	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. <ul style="list-style-type: none"> <li><b>[0]</b> 0 = (Default) Disable.</li> <li><b>[1]</b> 1 = Enable - previous voice payload packet is added to current packet.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>When enabled, you can configure the payload type, using the RFC2198PayloadType parameter.</li> <li>The RTP redundancy dynamic payload type can be included in the SDP, by using the EnableRTPRedundancyNegotiation parameter.</li> <li>This parameter can also be configured in an IP Profile.</li> </ul>
Web: Enable RTP Redundancy Negotiation	Enables the device to include the RTP redundancy dynamic payload type in the SDP, according to RFC 2198.

Parameter	Description
CLI: rtp-rdcy-nego-enbl <b>[EnableRTPRedundancyNegotiation]</b>	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>When enabled, the device includes in the SDP message the RTP payload type "RED" and the payload type configured by the parameter RFC2198PayloadType.</p> <pre>a=rtpmap:&lt;PT&gt; RED/8000</pre> <p>Where &lt;PT&gt; is the payload type as defined by RFC2198PayloadType. The device sends the INVITE message with "a=rtpmap:&lt;PT&gt; RED/8000" and responds with a 18x/200 OK and "a=rtpmap:&lt;PT&gt; RED/8000" in the SDP.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this feature to be functional, you must also set the parameter RTPRedundancyDepth to 1 (i.e., enabled).</li> <li>▪ Currently, the negotiation of "RED" payload type is not supported and therefore, it should be configured to the same PT value for both parties.</li> </ul>
Web: RFC 2198 Payload Type EMS: Redundancy Payload Type CLI: RTP-redundancy-payload-type <b>[RFC2198PayloadType]</b>	<p>Defines the RTP redundancy packet payload type according to RFC 2198.</p> <p>The range is 96 to 127. The default is 104.</p> <p><b>Note:</b> This parameter is applicable only if the parameter RTPRedundancyDepth is set to 1.</p>
Web: Packing Factor EMS: Packetization Factor <b>[RTPPackagingFactor]</b>	<p>N/A. Controlled internally by the device according to the selected coder.</p>
Web/EMS: Basic RTP Packet Interval <b>[BasicRTPPacketInterval]</b>	<p>N/A. Controlled internally by the device according to the selected coder.</p>
Web: RTP Directional Control <b>[RTPDirectionControl]</b>	<p>N/A. Controlled internally by the device according to the selected coder.</p>
Web/EMS: RFC 2833 TX Payload Type CLI: telephony-events-payload-type-tx <b>[RFC2833TxPayloadType]</b>	<p>Defines the Tx RFC 2833 DTMF relay dynamic payload type. The valid range is 96 to 99, and 106 to 127. The default is 96. The 100, 102 to 105 range is allocated for proprietary usage.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ Certain vendors (e.g., Cisco) use payload type 101 for RFC 2833.</li> <li>▪ When RFC 2833 payload type negotiation is used (i.e., the parameter TxDTMFOption 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.</li> </ul>
Web/EMS: RFC 2833 RX Payload Type CLI: telephony-events-payload-type-rx <b>[RFC2833RxPayloadType]</b>	<p>Defines the Rx RFC 2833 DTMF relay dynamic payload type. The valid range is 96 to 99, and 106 to 127. The default is 96. The 100, 102 to 105 range is allocated for proprietary usage.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ Certain vendors (e.g., Cisco) use payload type 101 for RFC 2833.</li> <li>▪ When RFC 2833 payload type negotiation is used (i.e., the parameter TxDTMFOption 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.</li> </ul>

Parameter	Description
<b>[EnableDetectRemoteMACChange]</b>	<p>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.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Nothing is changed.</li> <li>▪ <b>[1]</b> = 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.</li> <li>▪ <b>[2]</b> = (Default) The device uses the received GARP packets to change the MAC address of the transmitted RTP packets.</li> <li>▪ <b>[3]</b> = Options 1 and 2 are used.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ 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 this parameter to 0 or 2.</li> </ul>
Web: RTP Base UDP Port EMS: Base UDP Port <b>[BaseUDPport]</b>	<p>Defines the lower boundary of the UDP port used for RTP, RTCP (RTP port + 1) and T.38 (RTP port + 2). For example, if the Base UDP Port is set to 6000, then one channel may use the ports RTP 6000, RTCP 6001, and T.38 6002, while another channel may use RTP 6010, RTCP 6011, and T.38 6012, and so on.</p> <p>The range of possible UDP ports is 6,000 to 64,000. The default base UDP port is 6000.</p> <p>Once this parameter is configured, the UDP port range (lower to upper boundary) is calculated as follows:</p> <ul style="list-style-type: none"> <li>▪ BaseUDPport to (BaseUDPport + 255*10)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ The UDP ports are allocated randomly to channels.</li> <li>▪ You can define a UDP port range per Media Realm (see Configuring Media Realms on page 168).</li> <li>▪ If RTP Base UDP Port is not a factor of 10, the following message is generated: 'invalid local RTP port'.</li> </ul>
EMS: No Op Enable CLI: no-operation-enable <b>[NoOpEnable]</b>	<p>Enables the transmission of RTP or T.38 No-Op packets.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul> <p>This mechanism ensures that the NAT binding remains open during RTP or T.38 silence periods.</p>
EMS: No Op Interval <b>[NoOpInterval]</b>	<p>Defines the time interval in which RTP or T.38 No-Op packets are sent in the case of silence (no RTP/T.38 traffic) when No-Op packet transmission is enabled.</p> <p>The valid range is 20 to 65,000 msec. The default is 10,000.</p> <p><b>Note:</b> To enable No-Op packet transmission, use the NoOpEnable parameter.</p>

Parameter	Description
EMS: No Op Payload Type CLI: no-operation-interval <b>[RTPNoOpPayloadType]</b>	<p>Defines the payload type of No-Op packets.</p> <p>The valid range is 96 to 127 (for the range of Dynamic RTP Payload Type for all types of non hard-coded RTP Payload types, refer to RFC 3551). The default is 120.</p> <p><b>Note:</b> When defining this parameter, ensure that it doesn't cause collision with other payload types.</p>
CLI: rtcp-act-mode <b>[RTCPActivationMode]</b>	<p>Disables RTCP traffic when there is no RTP traffic. This feature is useful, for example, to stop RTCP traffic that is typically sent when calls are put on hold (by an INVITE with 'a=inactive' in the SDP).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Active Always = (Default) RTCP is active even during inactive RTP periods, i.e., when the media is in 'recvonly' or 'inactive' mode.</li> <li><b>[1]</b> Inactive Only If RTP Inactive = No RTCP is sent when RTP is inactive.</li> </ul>
<b>RTP Control Protocol Extended Reports (RTCP XR) Parameters</b>	
Web: Enable RTCP XR EMS: RTCP XR Enable CLI: voice-quality-monitoring-enable <b>[VQMonEnable]</b>	<p>Enables voice quality monitoring and RTCP XR, according to Internet-Draft draft-ietf-sipping-rtcp-summary-13.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Minimum Gap Size EMS: GMin <b>[VQMonGMin]</b>	<p>Defines the voice quality monitoring - minimum gap size (number of frames).</p> <p>The default is 16.</p>
Web/EMS: Burst Threshold <b>[VQMonBurstHR]</b>	<p>Defines the voice quality monitoring - excessive burst alert threshold.</p> <p>The default is -1 (i.e., no alerts are issued).</p>
Web/EMS: Delay Threshold <b>[VQMonDelayTHR]</b>	<p>Defines the voice quality monitoring - excessive delay alert threshold.</p> <p>The default is -1 (i.e., no alerts are issued).</p>
Web: R-Value Delay Threshold EMS: End of Call Rval Delay Threshold <b>[VQMonEOCRValTHR]</b>	<p>Defines the voice quality monitoring - end of call low quality alert threshold.</p> <p>The default is -1 (i.e., no alerts are issued).</p>
Web: RTCP XR Packet Interval EMS: Packet Interval CLI: rtcp-interval <b>[RTCPInterval]</b>	<p>Defines the time interval (in msec) between adjacent RTCP reports.</p> <p>The valid value range is 0 to 65,535. The default is 5,000.</p>
Web: Disable RTCP XR Interval Randomization EMS: Disable Interval Randomization CLI: disable-RTCP-randomization <b>[DisableRTCPRandomize]</b>	<p>Determines whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter RTCPInterval.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Randomize</li> <li><b>[1]</b> Enable = No Randomize</li> </ul>
EMS: RTCP XR Collection Server Transport Type <b>[RTCPXRESCTransportType]</b>	<p>Defines the transport layer used for outgoing SIP dialogs initiated by the device to the RTCP XR Collection Server.</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured (default)</li> <li><b>[0]</b> UDP</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[1]</b> TCP</li> <li>▪ <b>[2]</b> TLS</li> </ul> <p><b>Note:</b> When set to <b>[-1]</b>, the value of the SIPTransportType parameter is used.</p>
Web: RTCP XR Collection Server EMS: Esc IP CLI: rtcp-xr-coll-srvr <b>[RTCPXREscIP]</b>	Defines the IP address of the Event State Compositor (ESC). The device sends RTCP XR reports to this server, using SIP PUBLISH messages. The address can be configured as a numerical IP address or as a domain name.
Web: RTCP XR Report Mode EMS: Report Mode CLI: rtcp-xr-rep-mode <b>[RTCPXRReportMode]</b>	Determines whether RTCP XR reports are sent to the Event State Compositor (ESC) and defines the interval at which they are sent. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) RTCP XR reports are not sent to the ESC.</li> <li>▪ <b>[1]</b> End Call = RTCP XR reports are sent to the ESC at the end of each call.</li> <li>▪ <b>[2]</b> End Call &amp; Periodic = RTCP XR reports are sent to the ESC at the end of each call and periodically according to the RTCPInterval parameter.</li> </ul>

## 59.11 Gateway and IP-to-IP Parameters

### 59.11.1 Fax and Modem Parameters

The fax and modem parameters are described in the table below.

**Fax and Modem Parameters**

Parameter	Description
Web: Fax Transport Mode EMS: Transport Mode CLI: fax-transport-mode <b>[FaxTransportMode]</b>	Determines the fax transport mode used by the device. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = transparent mode</li> <li>▪ <b>[1]</b> T.38 Relay (default)</li> <li>▪ <b>[2]</b> Bypass</li> <li>▪ <b>[3]</b> Events Only</li> </ul> <p><b>Note:</b> This parameter is overridden by the parameter IsFaxUsed. If the parameter IsFaxUsed is set to 1 (T.38 Relay) or 3 (Fax Fallback), then FaxTransportMode is always set to 1 (T.38 relay).</p>
EMS: V34 Transport Method CLI: V34-fax-transport-type <b>[V34FaxTransportType]</b>	Determines the V.34 fax transport method (whether V34 fax falls back to T.30 or pass over Bypass). <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Transparent</li> <li>▪ <b>[1]</b> = (Default) Relay</li> <li>▪ <b>[2]</b> = Bypass</li> <li>▪ <b>[3]</b> = Transparent with Events</li> </ul> <p><b>Note:</b> To configure V34FaxTransportType to 1 (i.e., fax relay), you also need to configure FaxTransportMode to 1 (fax relay).</p>
Web: V.21 Modem Transport Type EMS: V21 Transport CLI: V21-modem-transport-	Determines the V.21 modem transport type. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) Disable (Transparent)</li> <li>▪ <b>[2]</b> Enable Bypass</li> </ul>

Parameter	Description
type <b>[V21ModemTransportType]</b>	<ul style="list-style-type: none"> <li><b>[3]</b> Events Only = Transparent with Events</li> </ul> <b>Note:</b> This parameter can also be configured in an IP Profile.
Web: V.22 Modem Transport Type EMS: V22 Transport CLI: V22-modem-transport-type <b>[V22ModemTransportType]</b>	Determines the V.22 modem transport type. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Disable (Transparent)</li> <li><b>[2]</b> Enable Bypass (default)</li> <li><b>[3]</b> Events Only = Transparent with Events</li> </ul> <b>Note:</b> This parameter can also be configured in an IP Profile.
Web: V.23 Modem Transport Type EMS: V23 Transport CLI: V23-modem-transport-type <b>[V23ModemTransportType]</b>	Determines the V.23 modem transport type. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Disable (Transparent)</li> <li><b>[2]</b> Enable Bypass (default)</li> <li><b>[3]</b> Events Only = Transparent with Events</li> </ul> <b>Note:</b> This parameter can also be configured in an IP Profile.
Web: V.32 Modem Transport Type EMS: V32 Transport CLI: V32-modem-transport-type <b>[V32ModemTransportType]</b>	Determines the V.32 modem transport type. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Disable (Transparent)</li> <li><b>[2]</b> Enable Bypass (default)</li> <li><b>[3]</b> Events Only = Transparent with Events</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter applies only to V.32 and V.32bis modems.</li> <li>This parameter can also be configured in an IP Profile.</li> </ul>
Web: V.34 Modem Transport Type EMS: V34 Transport CLI: V34-modem-transport-type <b>[V34ModemTransportType]</b>	Determines the V.90/V.34 modem transport type. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Disable (Transparent)</li> <li><b>[2]</b> Enable Bypass (default)</li> <li><b>[3]</b> Events Only = Transparent with Events</li> </ul> <b>Note:</b> This parameter can also be configured in an IP Profile.
EMS: Bell Transport Type CLI: bell-modem-transport-type <b>[BellModemTransportType]</b>	Determines the Bell modem transport method. <ul style="list-style-type: none"> <li><b>[0]</b> = Transparent (default)</li> <li><b>[2]</b> = Bypass</li> <li><b>[3]</b> = Transparent with events</li> </ul>
Web/EMS: Fax CNG Mode CLI: fax_cng_mode <b>[FaxCNGMode]</b>	Determines the device's handling of fax relay upon detection of a fax CNG tone or a V.34/Super G3 V8-CM (Call Menu) signal from originating faxes. <ul style="list-style-type: none"> <li><b>[0]</b> Doesn't send T.38 Re-INVITE = (Default) SIP re-INVITE is not sent.</li> <li><b>[1]</b> Sends on CNG tone = Sends a SIP re-INVITE with T.38 parameters in SDP to the terminating fax upon detection of a fax CNG tone, if the CNGDetectorMode parameter is set to 1.</li> <li><b>[2]</b> Sends on CNG or v8-cn = Sends a SIP re-INVITE with T.38 parameters in SDP to the terminating fax upon detection of a fax CNG tone (if the CNGDetectorMode parameter is set to 1) or upon detection of a V8-CM signal.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>If this parameter is set to <b>[2]</b> and the CNGDetectorMode parameter is set to <b>[0]</b>, the device sends a re-INVITE only if it detects a V8-CM signal from the originating fax.</li> <li>This feature is applicable only if the IsFaxUsed parameter is set to <b>[1]</b> or <b>[3]</b>.</li> <li>The device also sends T.38 re-INVITE if the CNGDetectorMode</li> </ul>



Parameter	Description
	parameter is set to <b>[2]</b> , regardless of the FaxCNGMode parameter settings.
Web/EMS: CNG Detector Mode CLI: coder <b>[CNGDetectorMode]</b>	<p>Determines whether the device detects the fax calling tone (CNG).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) The originating device doesn't detect CNG; the CNG signal passes transparently to the remote side.</li> <li>▪ <b>[1]</b> Relay = CNG is detected on the originating side. CNG packets are sent to the remote side according to T.38 (if IsFaxUsed = 1) and the fax session is started. A SIP Re-INVITE message isn't sent and the fax session starts by the terminating device. This option is useful, for example, 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 (i.e., originating device). To also send a Re-INVITE message upon detection of a fax CNG tone in this mode, set the parameter FaxCNGMode to 1 or 2.</li> <li>▪ <b>[2]</b> Events Only = CNG is detected on the originating side and a fax session is started by the originating side using the Re-INVITE message. Usually, T.38 fax session starts when the 'preamble' signal is detected by the answering side. Some SIP devices don't support the detection of this fax signal on the answering side and thus, in these cases it is possible to configure the device to start the T.38 fax session when the CNG tone is detected by the originating side. However, this mode is not recommended.</li> </ul> <p><b>Note:</b> This parameter can also be configured in an IP Profile.</p>
Web: SIP T38 Version CLI: sip-t38-ver <b>[SIPT38Version]</b>	<p>Determines the T.38 fax relay version.</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured = (Default) No T.38</li> <li>▪ <b>[0]</b> Version 0</li> <li>▪ <b>[3]</b> Version 3 = T.38 Version 3 (V.34 over T.38)</li> </ul> <p><b>Note:</b> For a description on V.34 over T.38 fax relay, see V.34 Fax Support on page 155.</p>
Web: Fax Relay Enhanced Redundancy Depth EMS: Enhanced Relay Redundancy Depth CLI: enhanced-redundancy-depth <b>[FaxRelayEnhancedRedundancyDepth]</b>	<p>Defines the number of times that control packets are retransmitted when using the T.38 standard.</p> <p>The valid range is 0 to 4. The default is 2.</p>
Web: Fax Relay Redundancy Depth EMS: Relay Redundancy Depth CLI: redundancy-depth <b>[FaxRelayRedundancyDepth]</b>	<p>Defines the number of times that each fax relay payload is retransmitted to the network.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) No redundancy</li> <li>▪ <b>[1]</b> = One packet redundancy</li> <li>▪ <b>[2]</b> = Two packet redundancy</li> </ul> <p><b>Note:</b> This parameter is applicable only to non-V.21 packets.</p>
Web: Fax Relay Max Rate (bps) EMS: Relay Max Rate CLI: max-rate <b>[FaxRelayMaxRate]</b>	<p>Defines the maximum rate (in bps) at which fax relay messages are transmitted (outgoing calls).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> 2400 = 2.4 kbps</li> <li>▪ <b>[1]</b> 4800 = 4.8 kbps</li> <li>▪ <b>[2]</b> 7200 = 7.2 kbps</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>[3] 9600 = 9.6 kbps</li> <li>[4] 12000 = 12.0 kbps</li> <li>[5] 14400 = 14.4 kbps (default)</li> <li>[6] 16800bps = 16.8 kbps</li> <li>[7] 19200bps = 19.2 kbps</li> <li>[8] 21600bps = 21.6 kbps</li> <li>[9] 24000bps = 24 kbps</li> <li>[10] 26400bps = 26.4 kbps</li> <li>[11] 28800bps = 28.8 kbps</li> <li>[12] 31200bps = 31.2 kbps</li> <li>[13] 33600bps = 33.6 kbps</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The rate is negotiated between both sides (i.e., the device adapts to the capabilities of the remote side). Negotiation of the T.38 maximum supported fax data rate is provided in SIP's SDP T38MaxBitRate parameter. The negotiated T38MaxBitRate is the minimum rate supported between the local and remote endpoints.</li> <li>Fax relay rates greater than 14.4 kbps are applicable only to V.34 / T.38 fax relay. For non-T.38 V.34 supporting devices, configuration greater than 14.4 kbps is truncated to 14.4 kbps.</li> </ul>
Web: Fax Relay ECM Enable EMS: Relay ECM Enable CLI: ecm-mode <b>[FaxRelayECMEnable]</b>	Enables Error Correction Mode (ECM) mode during fax relay. <ul style="list-style-type: none"> <li>[0] Disable</li> <li>[1] Enable (default)</li> </ul>
Web: Fax/Modem Bypass Coder Type EMS: Coder Type <b>[FaxModemBypassCoderType]</b>	Determines the coder used by the device when performing fax/modem bypass. Typically, high-bit-rate coders such as G.711 should be used. <ul style="list-style-type: none"> <li>[0] G.711Alaw= (Default) G.711 A-law 64</li> <li>[1] G.711Mulaw = G.711 <math>\mu</math>-law</li> </ul>
Web: Fax/Modem Bypass Packing Factor EMS: Packetization Period CLI: packing-factor <b>[FaxModemBypassM]</b>	Defines the number (20 msec) of coder payloads used to generate a fax/modem bypass packet.  The valid range is 1, 2, or 3 coder payloads. The default is 1 coder payload.
CLI: fax-modem-telephony- events-mode <b>[FaxModemNTEMode]</b>	Determines whether the device sends RFC 2833 ANS/ANSam events upon detection of fax and/or modem Answer tones (i.e., CED tone). <ul style="list-style-type: none"> <li>[0] = Disabled (default)</li> <li>[1] = Enabled</li> </ul> <p><b>Note:</b> This parameter is applicable only when the fax or modem transport type is set to bypass or Transparent-with-Events.</p>
Web/EMS: Fax Bypass Payload Type CLI: fax-bypass-payload-type <b>[FaxBypassPayloadType]</b>	Defines the fax bypass RTP dynamic payload type.  The valid range is 96 to 120. The default is 102.
EMS: Modem Bypass Payload Type CLI: modem-bypass-payload- type	Defines the modem bypass dynamic payload type.  The range is 0-127. The default is 103.



Parameter	Description
<b>[ModemBypassPayloadType]</b>	
EMS: Relay Volume (dBm) CLI: volume <b>[FaxModemRelayVolume]</b>	Defines the fax gain control. The range is -18 to -3, corresponding to -18 dBm to -3 dBm in 1-dB steps. The default is -6 dBm fax gain control.
Web/EMS: Fax Bypass Output Gain CLI: fax-bypass-output-gain <b>[FaxBypassOutputGain]</b>	Defines the fax bypass output gain control. The range is -31 to +31 dB, in 1-dB steps. The default is 0 (i.e., no gain).
Web/EMS: Modem Bypass Output Gain <b>[ModemBypassOutputGain]</b>	Defines the modem bypass output gain control. The range is -31 dB to +31 dB, in 1-dB steps. The default is 0 (i.e., no gain).
EMS: Basic Packet Interval CLI: modem-bypass-output-gain <b>[FaxModemBypassBasicRTP PacketInterval]</b>	Defines the basic frame size used during fax/modem bypass sessions. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Determined internally</li> <li>▪ <b>[1]</b> = 5 msec (not recommended)</li> <li>▪ <b>[2]</b> = 10 msec</li> <li>▪ <b>[3]</b> = 20 msec</li> </ul> <b>Note:</b> When set to 5 msec (1), the maximum number of simultaneous channels supported is 120.
EMS: Dynamic Jitter Buffer Minimal Delay (dB) CLI: jitter-buffer-minimum-delay <b>[FaxModemBypasDJBufMin Delay]</b>	Defines the Jitter Buffer delay (in milliseconds) during fax and modem bypass session. The range is 0 to 150 msec. The default is 40.
EMS: Enable Inband Network Detection CLI: enable-fax-modem-inband-network-detection <b>[EnableFaxModemInbandNetworkDetection]</b>	Enables in-band network detection related to fax/modem. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Disable.</li> <li>▪ <b>[1]</b> = Enable. When this parameter is enabled on Bypass and transparent with events mode (VxxTransportType is set to 2 or 3), a detection of an Answer Tone from the network triggers a switch to bypass mode in addition to the local Fax/Modem tone detections. However, only a high bit-rate coder voice session effectively detects the Answer Tone sent by a remote endpoint. This can be useful when, for example, the payload of voice and bypass is the same, allowing the originator to switch to bypass mode as well.</li> </ul>
EMS: NSE Mode CLI: NSE-mode <b>[NSEMode]</b>	Enables Cisco compatible fax and modem bypass mode. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) NSE disabled</li> <li>▪ <b>[1]</b> = NSE enabled</li> </ul> In NSE bypass mode, the device starts using G.711 A-Law (default) or G.711 $\mu$ -Law according to the FaxModemBypassCoderType parameter. The payload type used with these G.711 coders is a standard one (8 for G.711 A-Law and 0 for G.711 $\mu$ -Law). The parameters defining payload type for the 'old' Bypass mode FaxBypassPayloadType and ModemBypassPayloadType are not used with NSE Bypass. The bypass packet interval is selected according to the FaxModemBypassBasicRtpPacketInterval parameter.

Parameter	Description
	<p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This feature can be used only if the VxxModemTransportType parameter is set to 2 (Bypass).</li> <li>If NSE mode is enabled, the SDP contains the following line: 'a=rtpmap:100 X-NSE/8000'.</li> <li>To use this feature: <ul style="list-style-type: none"> <li>✓ The Cisco gateway must include the following definition: 'modem passthrough nse payload-type 100 codec g711alaw'.</li> <li>✓ Set the Modem transport type to Bypass mode (VxxModemTransportType is set to 2) for all modems.</li> <li>✓ Configure the gateway parameter NSEPayloadType = 100.</li> </ul> </li> <li>This parameter can also be configured in an IP Profile.</li> </ul>
EMS: NSE Payload Type CLI: nse-payload-type <b>[NSEPayloadType]</b>	<p>Defines the NSE payload type for Cisco Bypass compatible mode. The valid range is 96-127. The default is 105.</p> <p><b>Note:</b> Cisco gateways usually use NSE payload type of 100.</p>
EMS: T38 Use RTP Port <b>[T38UseRTPPort]</b>	<p>Defines the port (with relation to RTP port) for sending and receiving T.38 packets.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Use the RTP port +2 to send/receive T.38 packets.</li> <li><b>[1]</b> = Use the same port as the RTP port to send/receive T.38 packets.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, you must reset the device.</li> <li>When the device is configured to use V.152 to negotiate audio and T.38 coders, the UDP port published in SDP for RTP and for T38 must be different. Therefore, set the T38UseRTPPort parameter to 0.</li> </ul>
Web/EMS: T.38 Max Datagram Size CLI: t38-mx-datagram-sz <b>[T38MaxDatagramSize]</b>	<p>Defines the maximum size of a T.38 datagram that the device can receive. This value is included in the outgoing SDP when T.38 is used.</p> <p>The valid range is 120 to 600. The default is 560.</p>
Web/EMS: T38 Fax Max Buffer CLI: t38-fax-mx-buff <b>[T38FaxMaxBufferSize]</b>	<p>Defines the maximum size (in bytes) of the device's T.38 buffer. This value is included in the outgoing SDP when T.38 is used for fax relay over IP.</p> <p>The valid range is 500 to 3000. The default is 3000.</p>
Web: Detect Fax on Answer Tone EMS: Enables Detection of FAX on Answer Tone CLI: det-fax-on-ans-tone <b>[DetFaxOnAnswerTone]</b>	<p>Determines when the device initiates a T.38 session for fax transmission.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Initiate T.38 on Preamble = (Default) The device to which the called fax is connected initiates a T.38 session on receiving HDLC Preamble signal from the fax.</li> <li><b>[1]</b> Initiate T.38 on CED = The device to which the called fax is connected initiates a T.38 session on receiving a CED answer tone from the fax. This option can only be used to relay fax signals, as the device sends T.38 Re-INVITE on detection of any fax/modem Answer tone (2100 Hz, amplitude modulated 2100 Hz, or 2100 Hz with phase reversals). The modem signal fails when using T.38 for fax relay.</li> </ul> <p><b>Note:</b> This parameters is applicable only if the parameter IsFaxUsed is set to 1 (T.38 Relay) or 3 (Fax Fallback).</p>

Parameter	Description
<b>[CEDTransferMode]</b>	<p>Determines the fax CED tone transfer mode.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) The device transfers the CED tone in relay mode and starts the fax session immediately.</li> <li><b>[1]</b> = The device transfers the CED tone in either voice or bypass mode and starts the fax session on V21 preamble.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>This parameter is applicable only if the IsFaxUsed parameter is set to 1 (T.38 Relay).</li> </ul>
Web: T38 Fax Session Immediate Start CLI: t38-sess-imm-strt <b>[T38FaxSessionImmediateStart]</b>	<p>Enables fax transmission of T.38 "no-signal" packets to the terminating fax machine.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Immediate Start on Fax = Device activates T.38 fax relay upon receipt of a re-INVITE with T.38 only in the SDP.</li> <li><b>[2]</b> Immediate Start on Fax &amp; Voice = Device activates T.38 fax relay upon receipt of a re-INVITE with T.38 and audio media in the SDP.</li> </ul> <p>This parameter is used for transmission from fax machines connected to the device and located inside a NAT. Generally, the firewall blocks T.38 (and other) packets received from the WAN, unless the device behind 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.</p> <p>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.</p> <p><b>Note:</b> To enable No-Op packet transmission, use the NoOpEnable and NoOpInterval parameters.</p>
Web: Profile Number EMS: Allocation Profile <b>[V1501AllocationProfile]</b>	<p>Defines the V.150.1 profile, which determines how many DSP channels support V.150.1.</p> <p>The value range is 0 to 20. The default is 0.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web/EMS: SSE Payload Type Rx CLI: V1501-SSE-payload-type-rx <b>[V1501SSEPayloadTypeRx]</b>	<p>Defines the V.150.1 (modem relay protocol) State Signaling Event (SSE) payload type Rx.</p> <p>The value range is 96 to 127. The default is 105.</p>
Web/EMS: SSE Redundancy Depth CLI: SSE-redundancy-depth <b>[V1501SSERedundancyDepth]</b>	<p>Defines the SSE redundancy depth.</p> <p>The value range is 1-6. The default is 3.</p>
Web: SPRT Transport Ch.0 Max Payload Size CLI: SPRT-transport-channel0-max-payload-size <b>[V1501SPRTTransportChannel0MaxPayloadSize]</b>	<p>Defines the maximum payload size for V.150.1 SPRT Transport Channel 0.</p> <p>The range is 140 to 256. The default is 140.</p>

Parameter	Description
Web: SPRT Transport Ch.2 Max Payload Size CLI: SPRT-transport-channel2-max-payload-size <b>[V1501SPRTTransportChannel2MaxPayloadSize]</b>	Defines the maximum payload size for V.150.1 SPRT Transport Channel 2. The range is 132 to 256. The default is 132.
Web: SPRT Transport Ch.2 Max Window Size CLI: SPRT-transport-channel2-max-window-size <b>[V1501SPRTTransportChannel2MaxWindowSize]</b>	Defines the maximum window size of SPRT transport channel 2. The value range is 8 to 32. The default is 8.
Web: SPRT Transport Ch.3 Max Payload Size CLI: SPRT-transport-channel3-max-payload-size <b>[V1501SPRTTransportChannel3MaxPayloadSize]</b>	Defines the maximum payload size for V.150.1 SPRT Transport Channel 3. The range is 140 to 256. The default is 140.

## 59.11.2 DTMF and Hook-Flash Parameters

The DTMF and hook-flash parameters are described in the table below.

**DTMF and Hook-Flash Parameters**

Parameter	Description
<b>Hook-Flash Parameters</b>	
Web/EMS: Hook-Flash Code CLI: hook-flash-code <b>[HookFlashCode]</b>	For analog interfaces: Defines the digit pattern that when received from the Tel side, indicates a Hook Flash event. For digital interfaces: Defines the digit pattern used by the PBX to indicate a Hook Flash event. When this pattern is detected from the Tel side, the device responds as if a Hook Flash event has occurred and sends a SIP INFO message if the HookFlashOption parameter is set to 1, 5, 6, or 7 (indicating a Hook Flash). If configured and a Hook Flash indication is received from the IP side, the device generates this pattern to the Tel side. The valid range is a 25-character string. The default is a null string. <b>Note:</b> This parameter can also be configured in a Tel Profile.
Web/EMS: Hook-Flash Option CLI: hook-flash-option <b>[HookFlashOption]</b>	Determines the hook-flash transport type (i.e., method by which hook-flash is sent and received). For digital interfaces (E1/T1): This feature is applicable only if the HookFlashCode parameter is configured. <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = (Default) Hook-Flash indication is not sent.</li> <li><b>[1]</b> INFO = Sends proprietary INFO message (Broadsoft) with Hook-Flash indication. The device sends the INFO message as follows: <div style="background-color: #f0f0f0; padding: 5px;"> Content-Type: application/broadsoft; version=1.0  Content-Length: 17  event flashhook </div> </li> <li><b>[4]</b> RFC 2833 = This option is currently not supported.</li> <li><b>[5]</b> INFO (Lucent) = Sends proprietary SIP INFO message with</li> </ul>

Parameter	Description
	<p>Hook-Flash indication. The device sends the INFO message as follows:</p> <p>Content-Type: application/hook-flash Content-Length: 11 signal=hf</p> <ul style="list-style-type: none"> <li>▪ <b>[6] INFO (NetCentrex)</b> = Sends proprietary SIP INFO message with Hook-Flash indication. The device sends the INFO message as follows: Content-Type: application/dtmf-relay Signal=16 Where 16 is the DTMF code for hook flash.</li> <li>▪ <b>[7] INFO (HUAWAEI)</b> = Sends a SIP INFO message with Hook-Flash indication. The device sends the INFO message as follows: Content-Length: 17 Content-Type: application/sscc event=flashhook</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The device can interwork DTMF HookFlashCode to SIP INFO messages with Hook Flash indication (for digital interfaces).</li> <li>▪ FXO interfaces support only the receipt of RFC 2833 Hook-Flash signals and INFO <b>[1]</b> type.</li> <li>▪ FXS interfaces send Hook-Flash signals only if the EnableHold parameter is set to 0.</li> </ul>
<p>Web: Min. Flash-Hook Detection Period <b>[msec]</b> EMS: Min Flash Hook Time CLI: min-flash-hook-time <b>[MinFlashHookTime]</b></p>	<p>Defines the minimum time (in msec) for detection of a hook-flash event. Detection is guaranteed for hook-flash periods of at least 60 msec (when setting the minimum time to 25). Hook-flash signals that last a shorter period of time are ignored.</p> <p>The valid range is 25 to 300. The default is 300.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ This parameter is applicable only to FXS interfaces.</li> <li>▪ It's recommended to reduce the detection time by 50 msec from the desired value. For example, if you want to set the value to 200 msec, then enter 150 msec (i.e., 200 minus 50).</li> </ul>
<p>Web: Max. Flash-Hook Detection Period <b>[msec]</b> EMS: Flash Hook Period CLI: flash-hook-period <b>[FlashHookPeriod]</b></p>	<p>Defines the hook-flash period (in msec) for both Tel and IP sides (per device). For the IP side, it defines the hook-flash period that is reported to the IP.</p> <p>For the analog side, it defines the following:</p> <ul style="list-style-type: none"> <li>▪ FXS interfaces: <ul style="list-style-type: none"> <li>✓ Maximum hook-flash detection period. A longer signal is considered an off-hook or on-hook event.</li> <li>✓ Hook-flash generation period upon detection of a SIP INFO message containing a hook-flash signal.</li> </ul> </li> <li>▪ FXO interfaces: Hook-flash generation period.</li> </ul> <p>The valid range is 25 to 3,000. The default is 700.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, you need to reset the device.</li> <li>▪ For FXO interfaces, a constant of 100 msec must be added to the required hook-flash period. For example, to generate a 450 msec</li> </ul>

Parameter	Description
	hook-flash, set this parameter to 550. <ul style="list-style-type: none"> <li>This parameter can also be configured in a Tel Profile.</li> </ul>
<b>DTMF Parameters</b>	
EMS: Use End of DTMF CLI: notify-on-sig-end <b>[MGCPDTMFDetectionPoint]</b>	Determines when the detection of DTMF events is notified. <ul style="list-style-type: none"> <li><b>[0]</b> = DTMF event is reported at the end of a detected DTMF digit.</li> <li><b>[1]</b> = (Default) DTMF event is reported at the start of a detected DTMF digit.</li> </ul>
Web: Declare RFC 2833 in SDP EMS: Rx DTMF Option CLI: rfc-2833-in-sdp <b>[RxDTMFOption]</b>	Defines the supported receive DTMF negotiation method. <ul style="list-style-type: none"> <li><b>[0]</b> No = Don't declare RFC 2833 telephony-event parameter in SDP.</li> <li><b>[3]</b> Yes = (Default) Declare RFC 2833 telephony-event parameter in SDP.</li> </ul> <p>The device is always receptive to RFC 2833 DTMF relay packets. Therefore, it is always correct to include the 'telephony-event' parameter as default in the SDP. However, some devices use the absence of the 'telephony-event' in the SDP to decide to send DTMF digits in-band using G.711 coder. If this is the case, you can set this parameter to 0.</p> <p><b>Note:</b> This parameter can also be configured in an IP Profile.</p>
<b>Tx DTMF Option Table</b>	
Web/EMS: Tx DTMF Option CLI: configure voip > gw dtmf-and-suppl dtmf-and-dialing > dtmf-options <b>[TxDTMFOption]</b>	<p>This table parameter configures up to two preferred transmit DTMF negotiation methods. The format of this parameter is as follows:  <b>[TxDTMFOption]</b>  FORMAT TxDTMFOption_Index = TxDTMFOption_Type;  <b>[TxDTMFOption]</b></p> <p>Where Type is:</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = (Default) No negotiation - DTMF digits are sent according to the parameters DTMFTransportType and RFC2833PayloadType.</li> <li><b>[1]</b> INFO (Nortel) = Sends DTMF digits according to IETF Internet-Draft draft-choudhuri-sip-info-digit-00.</li> <li><b>[2]</b> NOTIFY = Sends DTMF digits according to IETF Internet-Draft draft-mahy-sipping-signaled-digits-01.</li> <li><b>[3]</b> INFO (Cisco) = Sends DTMF digits according to Cisco format.</li> <li><b>[4]</b> RFC 2833.</li> <li><b>[5]</b> INFO (Korea) = Sends DTMF digits according to Korea Telecom format.</li> </ul> <p>For example:  TxDTMFOption 0 = 1;  TxDTMFOption 1 = 3;</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>DTMF negotiation methods are prioritized according to the order of their appearance.</li> <li>When out-of-band DTMF transfer is used (<b>[1]</b>, <b>[2]</b>, <b>[3]</b>, or <b>[5]</b>), the parameter DTMFTransportType is automatically set to 0 (DTMF digits are erased from the RTP stream).</li> <li>When RFC 2833 (4) is selected, the device: <ol style="list-style-type: none"> <li>Negotiates RFC 2833 payload type using local and remote SDPs.</li> <li>Sends DTMF packets using RFC 2833 payload type according</li> </ol> </li> </ul>



Parameter	Description
	<p>to the payload type in the received SDP.</p> <ul style="list-style-type: none"> <li>c. Expects to receive RFC 2833 packets with the same payload type as configured by the parameter RFC2833PayloadType.</li> <li>d. Removes DTMF digits in transparent mode (as part of the voice stream).</li> </ul> <ul style="list-style-type: none"> <li>▪ When TxDTMFOption is set to 0, the RFC 2833 payload type is set according to the parameter RFC2833PayloadType for both transmit and receive.</li> <li>▪ If an ISDN phone user presses digits (e.g., for interactive voice response / IVR applications such as retrieving voice mail messages), ISDN Information messages received by the device for each digit are sent in the voice channel to the IP network as DTMF signals, according to the settings of the TxDTMFOption parameter.</li> <li>▪ The table ini file parameter TxDTMFOption can be repeated twice for configuring the DTMF transmit methods.</li> <li>▪ This parameter can also be configured in an IP Profile.</li> </ul>
<b>[DisableAutoDTMFMute]</b>	<p>Enables the automatic muting of DTMF digits when out-of-band DTMF transmission is used.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Automatic mute is used.</li> <li>▪ <b>[1]</b> = No automatic mute of in-band DTMF.</li> </ul> <p>When this parameter is set to 1, the DTMF transport type is set according to the parameter DTMFTransportType and the DTMF digits aren't muted if out-of-band DTMF mode is selected (TxDTMFOption set to 1, 2 or 3). This enables the sending of DTMF digits in-band (transparent of RFC 2833) in addition to out-of-band DTMF messages.</p> <p><b>Note:</b> Usually this mode is not recommended.</p>
Web/EMS: Enable Digit Delivery to IP CLI: digit-delivery-2ip <b>[EnableDigitDelivery2IP]</b>	<p>Enables the Digit Delivery feature whereby DTMF digits are sent to the destination IP address after the Tel-to-IP call is answered.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default).</li> <li>▪ <b>[1]</b> Enable = Enable digit delivery to IP.</li> </ul> <p>To enable this feature, modify the called number to include at least one 'p' character. The device uses the digits before the 'p' character in the initial INVITE message. After the call is answered, the device waits for the required time (number of 'p' multiplied by 1.5 seconds), and then sends the rest of the DTMF digits using the method chosen (in-band or out-of-band).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ The called number can include several 'p' characters (1.5 seconds pause), for example, 1001pp699, 8888p9p300.</li> </ul>
Web: Enable Digit Delivery to Tel EMS: Enable Digit Delivery CLI: digit-delivery-2tel <b>[EnableDigitDelivery]</b>	<p>Enables the Digit Delivery feature, which sends DTMF digits of the called number to the device's port (analog)/B-channel (digital) (phone line) after the call is answered (i.e., line is off-hooked for FXS, or seized for FXO) for IP-to-Tel calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default).</li> <li>▪ <b>[1]</b> Enable = Enable Digit Delivery feature for the FXO/FXS device.</li> </ul> <p>For digital interfaces: If the called number in IP-to-Tel call includes the characters 'w' or 'p', the device places a call with the first part of the called number (before 'w' or 'p') and plays DTMF digits after the call is answered. If the character 'w' is used, the device waits for detection of</p>

Parameter	Description
	<p>a dial tone before it starts playing DTMF digits. For example, if the called number is '1007766p100', the device places a call with 1007766 as the destination number, then after the call is answered it waits 1.5 seconds ('p') and plays the rest of the number (100) as DTMF digits.</p> <p>Additional examples: 1664wpp102, 66644ppp503, and 7774w100pp200.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For analog interfaces: The called number can include characters 'p' (1.5 seconds pause) and 'd' (detection of dial tone). If character 'd' is used, it must be the first 'digit' in the called number. The character 'p' can be used several times. For example (for FXS/FXO interfaces), the called number can be as follows: d1005, dpp699, p9p300. To add the 'd' and 'p' digits, use the usual number manipulation rules.</li> <li>For analog interfaces: To use this feature with FXO interfaces, configure the device to operate in one-stage dialing mode.</li> <li>If this parameter is enabled, it is possible to configure the FXS/FXO interface to wait for dial tone per destination phone number (before or during dialing of destination phone number). Therefore, the parameter <code>IsWaitForDialTone</code> (configurable for the entire device) is ignored.</li> <li>For analog interfaces: The FXS interface send SIP 200 OK responses only after the DTMF dialing is complete.</li> <li>This parameter can also be configured in a Tel Profile.</li> </ul>
CLI: replace-nb-sign-w-esc <b>[ReplaceNumberSignWithEscapeChar]</b>	<p>Determines whether to replace the number sign (#) with the escape character (%23) in outgoing SIP messages for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> Enable = All number signs #, received in the dialed DTMF digits are replaced in the outgoing SIP Request-URI and To headers with the escape sign %23.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only if the parameter <code>IsSpecialDigits</code> is set 1.</li> <li>This parameter is applicable only to analog interfaces.</li> </ul>
Web: Special Digit Representation EMS: Use Digit For Special DTMF CLI: special-digit-rep <b>[UseDigitForSpecialDTMF]</b>	<p>Defines the representation for 'special' digits ('*' and '#') that are used for out-of-band DTMF signaling (using SIP INFO/NOTIFY).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Special = (Default) Uses the strings '*' and '#'.</li> <li><b>[1]</b> Numeric = Uses the numerical values 10 and 11.</li> </ul>



### 59.11.3 Digit Collection and Dial Plan Parameters

The digit collection and dial plan parameters are described in the table below.

**Digit Collection and Dial Plan Parameters**

Parameter	Description
Web/EMS: Dial Plan Index CLI: dial-plan-index <b>[DialPlanIndex]</b>	<p>Defines the Dial Plan index to use in the external Dial Plan file. The Dial Plan file is loaded to the device as a .dat file (converted using the DConvert utility). The Dial Plan index can be defined globally or per Tel Profile.</p> <p>The valid value range is 0 to 7, where 0 denotes PLAN1, 1 denotes PLAN2, and so on. The default is -1, indicating that no Dial Plan file is used.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If this parameter is configured to select a Dial Plan index, the settings of the parameter DigitMapping are ignored.</li> <li>▪ If this parameter is configured to select a Dial Plan index from an external Dial Plan file, the device first attempts to locate a matching digit pattern in the Dial Plan file, and if not found, then attempts to locate a matching digit pattern in the Digit Map rules configured by the DigitMapping parameter.</li> <li>▪ This parameter is applicable also to ISDN with overlap dialing.</li> <li>▪ For E1 CAS MFC-R2 variants (which don't support terminating digit for the called party number, usually I-15), this parameter and the DigitMapping parameter are ignored. Instead, you can define a Dial Plan template per trunk using the parameter CasTrunkDialPlanName_x (or in the Trunk Settings page).</li> <li>▪ This parameter can also be configured in a Tel Profile.</li> <li>▪ For more information on the Dial Plan file, see 'Dialing Plans for Digit Collection' on page 542.</li> </ul>
CLI: tel2ip-src-nb-map-dial-index <b>[Tel2IPSourceNumberMappingDialPlanIndex]</b>	<p>Defines the Dial Plan index in the external Dial Plan file for the Tel-to-IP Source Number Mapping feature.</p> <p>The valid value range is 0 to 7, defining the Dial Plan index <b>[Plan x]</b> in the Dial Plan file. The default is -1 (disabled).</p> <p>For more information on this feature, see 'Modifying ISDN-to-IP Calling Party Number' on page 546.</p>
Web: Digit Mapping Rules EMS: Digit Map Patterns CLI: default-dm <b>[DigitMapping]</b>	<p>Defines the digit map pattern (used to reduce the dialing period when ISDN overlap dialing for digital interfaces). If the digit string (i.e., dialed number) matches one of the patterns in the digit map, the device stops collecting digits and establishes a call with the collected number.</p> <p>The digit map pattern can contain up to 52 options (rules), each separated by a vertical bar ( ). The maximum length of the entire digit pattern is 152 characters. The available notations include the following:</p> <ul style="list-style-type: none"> <li>▪ <b>[n-m]</b>: Range of numbers (not letters).</li> <li>▪ <b>.</b> (single dot): Repeat digits until next notation (e.g., T).</li> <li>▪ <b>x</b>: Any single digit.</li> <li>▪ <b>T</b>: Dial timeout (configured by the TimeBetweenDigits parameter).</li> <li>▪ <b>S</b>: Short timer (configured by the TimeBetweenDigits</li> </ul>

Parameter	Description
	<p>parameter; default is two seconds) that can be used when a specific rule is defined after a more general rule. For example, if the digit map is 99 998, then the digit collection is terminated after the first two 9 digits are received. Therefore, the second rule of 998 can never be matched. But when the digit map is 99s 998, then after dialing the first two 9 digits, the device waits another two seconds within which the caller can enter the digit 8.</p> <p>An example of a digit map is shown below: 11xS 00T [[1-7]xxx 8xxxxxxx #xxxxxxx]*xx 91xxxxxxxxx 9011x.T In the example above, the last rule can apply to International numbers: 9 for dialing tone, 011 Country Code, and then any number of digits for the local number ('x.').</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For ISDN interfaces, the digit map mechanism is applicable only when ISDN overlap dialing is used (ISDNRxOverlap is set to 1).</li> <li>If the DialPlanIndex parameter is configured (to select a Dial Plan index), then the device first attempts to locate a matching digit pattern in the Dial Plan file, and if not found, then attempts to locate a matching digit pattern in the Digit Map rules configured by the DigitMapping parameter.</li> <li>For more information on digit mapping, see 'Digit Mapping' on page 344.</li> </ul>
Web: Max Digits in Phone Num EMS: Max Digits in Phone Number CLI: mxdig-b4-dialing <b>[MaxDigits]</b>	<p>Defines the maximum number of collected destination number digits that can be received (i.e., dialed) from the Tel side (analog) when Tel-to-IP ISDN overlap dialing is performed (digital). When the number of collected digits reaches this maximum, the device uses these digits for the called destination number.</p> <p>The valid range is 1 to 49. The default is 5 for analog and 30 for digital.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Instead of using this parameter, Digit Mapping rules can be configured.</li> <li>Dialing ends when any of the following scenarios occur: <ul style="list-style-type: none"> <li>✓ Maximum number of digits is dialed</li> <li>✓ Interdigit Timeout (TimeBetweenDigits) expires</li> <li>✓ Pound (#) key is pressed</li> <li>✓ Digit map pattern is matched</li> </ul> </li> </ul>
Web: Inter Digit Timeout for Overlap Dialing <b>[sec]</b> EMS: Interdigit Timeout (Sec) CLI: time-btwn-dial-digs <b>[TimeBetweenDigits]</b>	<p>For analog interfaces: Defines the time (in seconds) that the device waits between digits that are dialed by the user.</p> <p>For ISDN overlap dialing: Defines the time (in seconds) that the device waits between digits that are received from the PSTN or IP during overlap dialing.</p> <p>When this inter-digit timeout expires, the device uses the collected digits to dial the called destination number.</p> <p>The valid range is 1 to 10. The default is 4.</p>
Web: Enable Special Digits EMS: Use '#' For Dial Termination CLI: special-digits <b>[IsSpecialDigits]</b>	<p>Determines whether the asterisk (*) and pound (#) digits can be used in DTMF.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Use '*' or '#' to terminate number collection (refer to the parameter UseDigitForSpecialDTMF). (Default.)</li> <li><b>[1]</b> Enable = Allows '*' and '#' for telephone numbers dialed by a</li> </ul>

Parameter	Description
	<p>user or for the endpoint telephone number.</p> <p><b>Note:</b> These symbols can always be used as the first digit of a dialed number even if you disable this parameter.</p>

### 59.11.4 Voice Mail Parameters

The voice mail parameters are described in the table below. For more information on the Voice Mail application, refer to the *CPE Configuration Guide for Voice Mail*.

#### Voice Mail Parameters

Parameter	Description															
Web/EMS: Voice Mail Interface CLI: vm-interface [VoiceMailInterface]	<p>Enables the device's Voice Mail application and determines the communication method used between the PBX and the device.</p> <ul style="list-style-type: none"><li>[0] None (default)</li><li>[1] DTMF</li><li>[2] SMDI</li><li>[3] QSIG</li><li>[4] SETUP Only = Applicable only to ISDN.</li><li>[5] MATRA/AASTRA QSIG</li><li>[6] QSIG SIEMENS = QSIG MWI activate and deactivate messages include Siemens Manufacturer Specific Information (MSI)</li><li>[7] IP2IP = The device's IP-to-IP application is used for interworking between an IP Voice Mail server and the device. This is implemented for sending unsolicited SIP NOTIFY messages received from the Voice Mail server to an IP Group (configured using the NotificationIPGroupID parameter).</li><li>[8] ETSI = Euro ISDN, according to ETS 300 745-1 V1.2.4, section 9.5.1.1. Enables MWI interworking from IP to Tel, typically used for BRI phones.</li></ul> <p><b>Note:</b> To disable voice mail per Trunk Group, you can use a Tel Profile with the EnableVoiceMailDelay parameter set to disabled (0). This eliminates the phenomenon of call delay on Trunks not implementing voice mail when voice mail is enabled using this global parameter.</p>															
Web: Enable VoiceMail URI EMS: Enable VMURI CLI: voicemail-uri [EnableVMURI]	<p>Enables the interworking of target and cause for redirection from Tel to IP and vice versa, according to RFC 4468.</p> <ul style="list-style-type: none"><li>[0] Disable (default)</li><li>[1] Enable</li></ul> <p>Upon receipt of an ISDN Setup message with Redirect values, the device maps the Redirect phone number to the SIP 'target' parameter and the Redirect number reason to the SIP 'cause' parameter in the Request-URI.</p> <table><tr><td>Redirecting Reason</td><td>&gt;&gt;</td><td>SIP Response Code</td></tr><tr><td>Unknown</td><td>&gt;&gt;</td><td>404</td></tr><tr><td>User busy</td><td>&gt;&gt;</td><td>486</td></tr><tr><td>No reply</td><td>&gt;&gt;</td><td>408</td></tr><tr><td>Deflection</td><td>&gt;&gt;</td><td>487/480</td></tr></table>	Redirecting Reason	>>	SIP Response Code	Unknown	>>	404	User busy	>>	486	No reply	>>	408	Deflection	>>	487/480
Redirecting Reason	>>	SIP Response Code														
Unknown	>>	404														
User busy	>>	486														
No reply	>>	408														
Deflection	>>	487/480														

Parameter	Description
	<p>Unconditional &gt;&gt; 302</p> <p>Others &gt;&gt; 302</p> <p>If the device receives a Request-URI that includes a 'target' and 'cause' parameter, the 'target' is mapped to the Redirect phone number and the 'cause' is mapped to the Redirect number reason.</p>
<b>[WaitForBusyTime]</b>	<p>Defines the time (in msec) that the device waits to detect busy and/or reorder tones. This feature is used for semi-supervised PBX call transfers (i.e., the LineTransferMode parameter is set to 2).</p> <p>The valid value range is 0 to 20000 (i.e., 20 sec). The default is 2000 (i.e., 2 sec).</p>
Web/EMS: Line Transfer Mode CLI: line-transfer-mode <b>[LineTransferMode]</b>	<p>Defines the call transfer method used by the device. This parameter is applicable to FXO call transfer as well as E1/T1 CAS call transfer if the TrunkTransferMode_x parameter is set to 3 (CAS Normal) or 1 (CAS NFA).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> None = (Default) IP.</li> <li>▪ <b>[1]</b> Blind = PBX blind transfer: <ul style="list-style-type: none"> <li>✓ Analog (FXO): After receiving a SIP REFER message from the IP side, the device (FXO) sends a hook-flash to the PBX, dials the digits (that are received in the Refer-To header), and then immediately releases the line (i.e., on-hook). The PBX performs the transfer internally.</li> <li>✓ E1/T1 CAS: When a SIP REFER message is received, the device performs a blind transfer, by performing a CAS wink, waiting a user-defined time (configured by the WaitForDialTime parameter), dialing the Refer-To number, and then releasing the call. The PBX performs the transfer internally.</li> </ul> </li> <li>▪ <b>[2]</b> Semi Supervised = PBX semi-supervised transfer: <ul style="list-style-type: none"> <li>✓ Analog (FXO): After receiving a SIP REFER message from the IP side, the device sends a hook-flash to the PBX, and then dials the digits (that are received in the Refer-To header). If no busy or reorder tones are detected (within the user-defined interval set by the WaitForBusyTime parameter), the device completes the call transfer by releasing the line. If these tones are detected, the transfer is cancelled, the device sends a SIP NOTIFY message with a failure reason in the NOTIFY body (such as 486 if busy tone detected), and generates an additional hook-flash toward the FXO line to restore connection to the original call.</li> <li>✓ E1/T1 CAS: The device performs a CAS wink, waits a user-defined time (configured by the WaitForDialTime parameter), and then dials the Refer-To number. If during the user-defined interval set by the WaitForBusyTime parameter, no busy or reorder tones are detected, the device completes the call transfer by releasing the line. If during this interval, the device detects these tones, the transfer operation is cancelled, the device sends a SIP NOTIFY message with a failure reason (e.g., 486 if a busy tone is detected), and then generates an additional wink toward the CAS line to restore connection with the original call.</li> </ul> </li> <li>▪ <b>[3]</b> Supervised = PBX Supervised transfer: <ul style="list-style-type: none"> <li>✓ Analog (FXO): After receiving a SIP REFER message from the IP side, the device sends a hook-flash to the PBX, and then</li> </ul> </li> </ul>

Parameter	Description
	<p>dials the digits (that are received in the Refer-To header). The device waits for connection of the transferred call and then completes the call transfer by releasing the line. If speech is not detected, the transfer is cancelled, the device sends a SIP NOTIFY message with a failure reason in the NOTIFY body (such as 486 if busy tone detected) and generates an additional hook-flash toward the FXO line to restore connection to the original call.</p> <p>✓ E1/T1 CAS: The device performs a supervised transfer to the PBX. The device performs a CAS wink, waits a user-defined time (configured by the WaitForDialTime parameter), and then dials the Refer-To number. The device completes the call transfer by releasing the line only after detection of the transferred party answer. To enable answer supervision, you also need to do the following:</p> <ol style="list-style-type: none"> <li>1) Enable voice detection (i.e., set the EnableVoiceDetection parameter to 1).</li> <li>2) Set the EnableDSIPMDetectors parameter to 1.</li> <li>3) Install the IPMDetector DSP option Software License Key.</li> </ol>
<b>SMDI Parameters</b>	
Web/EMS: Enable SMDI <b>[SMDI]</b>	<p>Enables Simplified Message Desk Interface (SMDI) interface on the device.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) Normal serial</li> <li>▪ <b>[1]</b> Enable (Bellcore)</li> <li>▪ <b>[2]</b> Ericsson MD-110</li> <li>▪ <b>[3]</b> NEC (ICS)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ When the RS-232 connection is used for SMDI messages (Serial SMDI), it cannot be used for other applications, for example, to access the Command Line Interface (CLI).</li> </ul>
Web/EMS: SMDI Timeout <b>[SMDITimeOut]</b>	<p>Defines the time (in msec) that the device waits for an SMDI Call Status message before or after a Setup message is received. This parameter synchronizes the SMDI and analog CAS interfaces.</p> <p>If the timeout expires and only an SMDI message is received, the SMDI message is dropped. If the timeout expires and only a Setup message is received, the call is established.</p> <p>The valid range is 0 to 10000 (i.e., 10 seconds). The default is 2000.</p>
<b>Message Waiting Indication (MWI) Parameters</b>	
Web: MWI Off Digit Pattern EMS: MWI Off Code CLI: mwi-off-dig-ptn <b>[MWIOffCode]</b>	<p>Defines the digit code used by the device to notify the PBX that there are no messages waiting for a specific extension. This code is added as prefix to the dialed number.</p> <p>The valid range is a 25-character string.</p>
Web: MWI On Digit Pattern EMS: MWI On Code CLI: mwi-on-dig-ptn <b>[MWIONCode]</b>	<p>Defines the digit code used by the device to notify the PBX of messages waiting for a specific extension. This code is added as prefix to the dialed number.</p> <p>The valid range is a 25-character string.</p>

Parameter	Description
Web: MWI Suffix Pattern EMS: MWI Suffix Code CLI: mwi-suffix-pattern <b>[MWISuffixCode]</b>	Defines the digit code used by the device as a suffix for 'MWI On Digit Pattern' and 'MWI Off Digit Pattern'. This suffix is added to the generated DTMF string after the extension number. The valid range is a 25-character string.
Web: MWI Source Number EMS: MWI Source Name CLI: mwi-source-number <b>[MWISourceNumber]</b>	Defines the calling party's phone number used in the Q.931 MWI Setup message to PSTN. If not configured, the channel's phone number is used as the calling number.
CLI: mwi-subscribe-ipgrp-id <b>[MWISubscribeIPGroupID]</b>	Defines the IP Group ID used when subscribing to an MWI server. The 'The SIP Group Name' field value of the IP Group table is used as the Request-URI host name in the outgoing MWI SIP SUBSCRIBE message. The request is sent to the IP address defined for the Proxy Set that is associated with the IP Group. The Proxy Set's capabilities such as proxy redundancy and load balancing are also applied to the message.  For example, if the 'SIP Group Name' field of the IP Group is set to "company.com", the device sends the following SUBSCRIBE message: <pre>SUBSCRIBE sip:company.com...</pre> Instead of: <pre>SUBSCRIBE sip:10.33.10.10...</pre> <b>Note:</b> If this parameter is not configured, the MWI SUBSCRIBE message is sent to the MWI server as defined by the MWIServerIP parameter.
<b>[NotificationIPGroupID]</b>	Defines the IP Group ID to which the device sends SIP NOTIFY MWI messages. <b>Notes:</b> <ul style="list-style-type: none"> <li>This is used for MWI Interrogation. For more information on the interworking of QSIG MWI to IP, see Message Waiting Indication on page 358.</li> <li>To determine the handling method of MWI Interrogation messages, use the TrunkGroupSettings_MWIIterrogationType, parameter (in the Trunk Group Settings table).</li> </ul>
<b>[MWIQsigMsgCentredID PartyNumber]</b>	Defines the Message Centred ID party number used for QSIG MWI messages. If not configured (default), the parameter is not included in MWI (activate and deactivate) QSIG messages. The valid value is a string.
<b>Digit Patterns</b> The following digit pattern parameters apply only to voice mail applications that use the DTMF communication method. For the available pattern syntaxes, refer to the <i>CPE Configuration Guide for Voice Mail</i> .	
Web: Forward on Busy Digit Pattern (Internal) EMS: Digit Pattern Forward On Busy CLI: fwd-busy-dig-ptn-int <b>[DigitPatternForwardOn Busy]</b>	Defines the digit pattern used by the PBX to indicate 'call forward on busy' when the original call is received from an internal extension. The valid range is a 120-character string.

Parameter	Description
Web: Forward on No Answer Digit Pattern (Internal) EMS: Digit Pattern Forward On No Answer CLI: fwd-no-ans-dig-pat-int <b>[DigitPatternForwardOnNoAnswer]</b>	Defines the digit pattern used by the PBX to indicate 'call forward on no answer' when the original call is received from an internal extension.  The valid range is a 120-character string.
Web: Forward on Do Not Disturb Digit Pattern (Internal) EMS: Digit Pattern Forward On DND CLI: fwd-dnd-dig-ptn-int <b>[DigitPatternForwardOnDND]</b>	Defines the digit pattern used by the PBX to indicate 'call forward on do not disturb' when the original call is received from an internal extension.  The valid range is a 120-character string.
Web: Forward on No Reason Digit Pattern (Internal) EMS: Digit Pattern Forward No Reason CLI: fwd-no-rsn-dig-ptn-int <b>[DigitPatternForwardNoReason]</b>	Defines the digit pattern used by the PBX to indicate 'call forward with no reason' when the original call is received from an internal extension.  The valid range is a 120-character string.
Web: Forward on Busy Digit Pattern (External) EMS: VM Digit Pattern On Busy External CLI: fwd-bsy-dig-ptn-ext <b>[DigitPatternForwardOnBusyExt]</b>	Defines the digit pattern used by the PBX to indicate 'call forward on busy' when the original call is received from an external line (not an internal extension).  The valid range is a 120-character string.
Web: Forward on No Answer Digit Pattern (External) EMS: VM Digit Pattern On No Answer Ext CLI: fwd-no-ans-dig-pat-ext <b>[DigitPatternForwardOnNoAnswerExt]</b>	Defines the digit pattern used by the PBX to indicate 'call forward on no answer' when the original call is received from an external line (not an internal extension).  The valid range is a 120-character string.
Web: Forward on Do Not Disturb Digit Pattern (External) EMS: VM Digit Pattern On DND External CLI: fwd-dnd-dig-ptn-ext <b>[DigitPatternForwardOnDNDExt]</b>	Defines the digit pattern used by the PBX to indicate 'call forward on do not disturb' when the original call is received from an external line (not an internal extension).  The valid range is a 120-character string.



Parameter	Description
Web: Forward on No Reason Digit Pattern (External) EMS: VM Digit Pattern No Reason External CLI: fwd-no-rsn-dig-ptn-ext <b>[DigitPatternForwardNoReasonExt]</b>	Defines the digit pattern used by the PBX to indicate 'call forward with no reason' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Web: Internal Call Digit Pattern EMS: Digit Pattern Internal Call CLI: int-call-dig-ptn <b>[DigitPatternInternalCall]</b>	Defines the digit pattern used by the PBX to indicate an internal call. The valid range is a 120-character string.
Web: External Call Digit Pattern EMS: Digit Pattern External Call CLI: ext-call-dig-ptn <b>[DigitPatternExternalCall]</b>	Defines the digit pattern used by the PBX to indicate an external call. The valid range is a 120-character string.
Web: Disconnect Call Digit Pattern EMS: Tel Disconnect Code CLI: disc-call-dig-ptn <b>[TelDisconnectCode]</b>	Defines a digit pattern that when received from the Tel side, indicates the device to disconnect the call. The valid range is a 25-character string.
Web: Digit To Ignore Digit Pattern EMS: Digit To Ignore CLI: dig-to-ignore-dig-pattern <b>[DigitPatternDigitToIgnore]</b>	Defines a digit pattern that if received as Src (S) or Redirect (R) numbers is ignored and not added to that number. The valid range is a 25-character string.



## 59.11.5 Supplementary Services Parameters

This subsection describes the device's supplementary telephony services parameters.

### 59.11.5.1 Caller ID Parameters

The caller ID parameters are described in the table below.

**Caller ID Parameters**

Parameter	Description
Caller ID Permissions Table	
Web: Caller ID Permissions Table EMS: SIP Endpoints > Caller ID CLI: configure voip > gw analoggw enable-caller-id <b>[EnableCallerID]</b>	<p>This table parameter enables (per port) Caller ID generation (for FXS interfaces) and detection (for FXO interfaces). The format of this parameter is as follows:</p> <p><b>[EnableCallerID]</b>            FORMAT EnableCallerID_Index = EnableCallerID_IsEnabled, EnableCallerID_Module, EnableCallerID_Port;  <b>[EnableCallerID]</b></p> <p>Where,</p> <ul style="list-style-type: none"> <li>Module = Module number, where 1 denotes the module in Slot 1.</li> <li>Port = Port number, where 1 denotes Port 1 of a module.</li> </ul> <p>For example:            EnableCallerID 0 = 1,3,1; (caller ID enabled on Port 1 of Module 3)            EnableCallerID 1 = 0,3,2; (caller ID disabled on Port 2 of Module 3)</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The indexing of this parameter starts at 0.</li> <li>For a detailed description of this table, see Configuring Caller ID Permissions on page 401.</li> </ul>
Caller Display Information Table	
Web: Caller Display Information Table EMS: SIP Endpoints > Caller ID CLI: configure voip > gw analoggw caller-display-info <b>[CallerDisplayInfo]</b>	<p>This table parameter enables the device to send Caller ID information to the IP side when a call is made. The called party can use this information for caller identification. The information configured in this table is sent in the SIP INVITE message's From header. The format of this parameter is as follows:</p> <p><b>[CallerDisplayInfo]</b>            FORMAT CallerDisplayInfo_Index = CallerDisplayInfo_DisplayString, CallerDisplayInfo_IsCidRestricted, CallerDisplayInfo_Module, CallerDisplayInfo_Port;  <b>[CallerDisplayInfo]</b></p> <p>Where,</p> <ul style="list-style-type: none"> <li>Module = Module number, where 1 denotes the module in Slot 1.</li> <li>Port = Port number, where 1 denotes Port 1 of a module.</li> </ul> <p>For example:            CallerDisplayInfo 0 = Susan C.,0,1,1; ("Susan C." is sent as the Caller ID for Port 1 of Module 1)            CallerDisplayInfo 1 = Mark M.,0,1,2; ("Mark M." is sent as Caller ID for Port 2 of Module 1)</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The indexing of this table ini file parameter starts at 0.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>For a detailed description of this table, see Configuring Caller Display Information on page 398.</li> </ul>
Web/EMS: Enable Caller ID CLI: enable-caller-id <b>[EnableCallerID]</b>	<p>Enables Caller ID.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>If the Caller ID service is enabled, then for FXS interfaces, calling number and Display text (from IP) are sent to the device's port. For FXO interfaces, the Caller ID signal is detected and sent to IP in the SIP INVITE message (as 'Display' element). For information on the Caller ID table, see Configuring Caller Display Information on page 398. To disable/enable caller ID generation per port, see Configuring Call Forward on page 399.</p>
Web: Caller ID Type EMS: Caller id Types CLI: caller-ID-type <b>[CallerIDType]</b>	<p>Determines the standard used for detection (FXO) and generation (FXS) of Caller ID, and detection (FXO) / generation (FXS) of MWI (when specified) signals:</p> <ul style="list-style-type: none"> <li><b>[0]</b> Standard Bellcore = (Default) Caller ID and MWI</li> <li><b>[1]</b> Standard ETSI = Caller ID and MWI</li> <li><b>[2]</b> Standard NTT</li> <li><b>[4]</b> Standard BT = Britain</li> <li><b>[16]</b> Standard DTMF Based ETSI</li> <li><b>[17]</b> Standard Denmark = Caller ID and MWI</li> <li><b>[18]</b> Standard India</li> <li><b>[19]</b> Standard Brazil</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Typically, the Caller ID signals are generated/detected between the first and second rings. However, sometimes the Caller ID is detected before the first ring signal. In such a scenario, set the RingsBeforeCallerID parameter to 0.</li> <li>Caller ID detection for Britain <b>[4]</b> is not supported on the device's FXO ports. Only FXS ports can generate the Britain <b>[4]</b> Caller ID.</li> <li>To select the Bellcore Caller ID sub standard, use the BellcoreCallerIDTypeOneSubStandard parameter. To select the ETSI Caller ID substandard, use the ETSICallerIDTypeOneSubStandard parameter.</li> <li>To select the Bellcore MWI sub standard, use the BellcoreVMWITypeOneStandard parameter. To select the ETSI MWI sub standard, use the ETSIVMWITypeOneStandard parameter.</li> <li>If you define Caller ID Type as NTT <b>[2]</b>, you need to define the NTT DID signaling form (FSK or DTMF) using the NTTDIDSignallingForm parameter.</li> </ul>
Web: Enable FXS Caller ID Category Digit For Brazil Telecom CLI: fxs-callid-cat-brazil <b>[AddCPCPrefix2BrazilCallerID]</b>	<p>Enables the interworking of Calling Party Category (cpc) code from SIP INVITE messages to FXS Caller ID first digit.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>When this parameter is enabled, the device sends the Caller ID number (calling number) with the cpc code (received in the SIP INVITE message) to the device's FXS port. The cpc code is added as a prefix to the caller ID (after IP-to-Tel calling number manipulation). For example, assuming that the incoming INVITE contains the following</p>

Parameter	Description																											
	<p>From (or P-Asserted-Id) header: From:&lt;sip:+551137077801;cpc=payphone@10.20.7.35&gt;;tag=53700</p> <p>The calling number manipulation removes "+55" (leaving 10 digits), and then adds the prefix 7, the cpc code for payphone user. Therefore, the Caller ID number that is sent to the FXS port, in this example is 71137077801.</p> <p>If the incoming INVITE message doesn't contain the 'cpc' parameter, nothing is added to the Caller ID number.</p> <table><tr><th>CPC Value in Received INVITE</th><th>CPC Code Prefixed to Caller ID (Sent to FXS Endpoint)</th><th>Description</th></tr><tr><td>cpc=unknown</td><td>1</td><td>Unknown user</td></tr><tr><td>cpc=subscribe</td><td>1</td><td>-</td></tr><tr><td>cpc=ordinary</td><td>1</td><td>Ordinary user</td></tr><tr><td>cpc=priority</td><td>2</td><td>Pre-paid user</td></tr><tr><td>cpc=test</td><td>3</td><td>Test user</td></tr><tr><td>cpc=operator</td><td>5</td><td>Operator</td></tr><tr><td>cpc=data</td><td>6</td><td>Data call</td></tr><tr><td>cpc=payphone</td><td>7</td><td>Payphone user</td></tr></table> <p><b>Notes:</b></p> <ul style="list-style-type: none"><li>▪ This parameter is applicable only to FXS interfaces.</li><li>▪ For this parameter to be enabled, you must also set the parameter EnableCallingPartyCategory to 1.</li></ul>	CPC Value in Received INVITE	CPC Code Prefixed to Caller ID (Sent to FXS Endpoint)	Description	cpc=unknown	1	Unknown user	cpc=subscribe	1	-	cpc=ordinary	1	Ordinary user	cpc=priority	2	Pre-paid user	cpc=test	3	Test user	cpc=operator	5	Operator	cpc=data	6	Data call	cpc=payphone	7	Payphone user
CPC Value in Received INVITE	CPC Code Prefixed to Caller ID (Sent to FXS Endpoint)	Description																										
cpc=unknown	1	Unknown user																										
cpc=subscribe	1	-																										
cpc=ordinary	1	Ordinary user																										
cpc=priority	2	Pre-paid user																										
cpc=test	3	Test user																										
cpc=operator	5	Operator																										
cpc=data	6	Data call																										
cpc=payphone	7	Payphone user																										
[EnableCallerIDTypeTwo]	<p>Disables the generation of Caller ID type 2 when the phone is off-hooked. Caller ID type 2 (also known as off-hook Caller ID) is sent to a currently busy telephone to display the caller ID of the waiting call.</p> <ul style="list-style-type: none"><li>▪ [0] = Caller ID type 2 isn't played.</li><li>▪ [1] = (Default) Caller ID type 2 is played.</li></ul>																											
EMS: Caller ID Timing Mode CLI: caller-id-timing-mode [AnalogCallerIDTimingMode]	<p>Determines when Caller ID is generated.</p> <ul style="list-style-type: none"><li>▪ [0] = (Default) Caller ID is generated between the first two rings.</li><li>▪ [1] = The device attempts to find an optimized timing to generate the Caller ID according to the selected Caller ID type.</li></ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"><li>▪ This parameter is applicable only to FXS interfaces.</li><li>▪ If this parameter is set to 1 and used with distinctive ringing, the Caller ID signal doesn't change the distinctive ringing timing.</li><li>▪ For this parameter to take effect, a device reset is required.</li></ul>																											
EMS: Bellcore Caller ID Type One Sub Standard CLI: bellcore-callerid-type-one-sub-standard [BellcoreCallerIDTypeOneSubStandard]	<p>Determines the Bellcore Caller ID sub-standard.</p> <ul style="list-style-type: none"><li>▪ [0] = (Default) Between rings.</li><li>▪ [1] = Not ring related.</li></ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>																											

Parameter	Description
EMS: ETSI Caller ID Type One Sub Standard CLI: etsi-callerid-type-one-sub-standard <b>[ETSICallerIDTypeOneSubStandard]</b>	<p>Determines the ETSI FSK Caller ID Type 1 sub-standard (FXS only).</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) ETSI between rings.</li> <li><b>[1]</b> = ETSI before ring DT_AS.</li> <li><b>[2]</b> = ETSI before ring RP_AS.</li> <li><b>[3]</b> = ETSI before ring LR_DT_AS.</li> <li><b>[4]</b> = ETSI not ring related DT_AS.</li> <li><b>[5]</b> = ETSI not ring related RP_AS.</li> <li><b>[6]</b> = ETSI not ring related LR_DT_AS.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Asserted Identity Mode EMS: Asserted ID Mode CLI: asserted-identity-m <b>[AssertedIdMode]</b>	<p>Determines whether the SIP header P-Asserted-Identity or P-Preferred-Identity is used in the generated SIP INVITE, 200 OK, or UPDATE request for Caller ID (or privacy). These headers are used to present the originating party's Caller ID. The Caller ID is composed of a Calling Number and a Calling Name (optional).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disabled = (Default) P-Asserted-Identity nor P-Preferred-Identity headers are not added.</li> <li><b>[1]</b> Add P-Asserted-Identity</li> <li><b>[2]</b> Add P-Preferred-Identity</li> </ul> <p>The header used also depends on the calling Privacy (allowed or restricted). These headers are used together with the Privacy header. If Caller ID is restricted (i.e., P-Asserted-Identity is not sent), the Privacy header includes the value 'id' ('Privacy: id'). Otherwise, for allowed Caller ID, 'Privacy: none' is used. If Caller ID is restricted (received from PSTN / Tel or configured in the device), the From header is set to &lt;anonymous@anonymous.invalid&gt;.</p> <p>The 200 OK response can contain the connected party CallerID - Connected Number and Connected Name. For example, if the call is answered by the device, the 200 OK response includes the P-Asserted-Identity with Caller ID. The device interworks (in some ISDN variants), the Connected Party number and name from Q.931 Connect message to SIP 200 OK with the P-Asserted-Identity header. In the opposite direction, if the ISDN device receives a 200 OK with P-Asserted-Identity header, it interworks it to the Connected party number and name in the Q.931 Connect message, including its privacy.</p>
Web/EMS: Use Destination As Connected Number <b>[UseDestinationAsConnectedNumber]</b>	<p>Enables the device to include the Called Party Number, from outgoing Tel calls (after number manipulation), in the SIP P-Asserted-Identity header. The device includes the SIP P-Asserted-Identity header in 180 Ringing and 200 OK responses for IP-to-Tel calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this feature, you must also enable the device to include the P-Asserted-Identity header in 180/200 OK responses, by setting the parameter AssertedIDMode to <b>Add P-Asserted-Identity</b>.</li> <li>If the received Q.931 Connect message contains a Connected Party Number, this number is used in the P-Asserted-Identity header in 200 OK response.</li> <li>This parameter is applicable to ISDN, CAS, and/or FXO interfaces.</li> </ul>
Web: Caller ID Transport Type	<p>Determines the device's behavior for Caller ID detection.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = The caller ID signal is not detected - DTMF digits</li> </ul>

Parameter	Description
EMS: Transport Type CLI: caller-ID-transport-type <b>[CallerIDTransportType]</b>	<p>remain in the voice stream.</p> <ul style="list-style-type: none"> <li><b>[1]</b> Relay = (Currently not applicable.)</li> <li><b>[3]</b> Mute = (Default) The caller ID signal is detected from the Tel/PSTN side and then erased from the voice stream.</li> </ul> <p><b>Note:</b> Caller ID detection is applicable only to FXO interfaces.</p>
<b>Reject Anonymous Calls Per Port Table</b>	
CLI: configure voip > gw analoggw reject-anonymous-calls <b>[RejectAnonymousCallPerPort]</b>	<p>This table parameter determines whether the device rejects incoming anonymous calls per FXS port. If enabled, when a device's FXS interface receives an anonymous call, it rejects the call and responds with a SIP 433 (Anonymity Disallowed) response.</p> <p>The format of this parameter is as follows:</p> <p><b>[RejectAnonymousCallPerPort]</b>  FORMAT RejectAnonymousCallPerPort_Index =  RejectAnonymousCallPerPort_Enable,  RejectAnonymousCallPerPort_Port,  RejectAnonymousCallPerPort_Module;  <b>[RejectAnonymousCallPerPort]</b></p> <p>Where,</p> <ul style="list-style-type: none"> <li>Enable = accept <b>[0]</b> (default) or reject <b>[1]</b> incoming anonymous calls.</li> <li>Port = Port number.</li> <li>Module = Module number.</li> </ul> <p>For example:  RejectAnonymousCallPerPort 0 = 0,1,1;  RejectAnonymousCallPerPort 1 = 1,2,1;</p> <p><b>Note:</b> This parameter is applicable only to FXS interfaces.</p>

### 59.11.5.2 Call Waiting Parameters

The call waiting parameters are described in the table below.

**Call Waiting Parameters**

Parameter	Description
Web/EMS: Enable Call Waiting CLI: call-waiting <b>[EnableCallWaiting]</b>	<p>Enables the Call Waiting feature.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (Default)</li> </ul> <p>For digital interfaces: If enabled and the device initiates a Tel-to-IP call to a destination that is busy, it plays a call waiting ringback tone to the caller. The tone is played only if the destination returns a 182 "Queued" SIP response.</p> <p>For FXS interface: If enabled, when an FXS interface receives a call on a busy endpoint, it responds with a 182 response (and not with a 486 busy). The device plays a call waiting indication signal. When hook-flash is detected, the device switches to the waiting call. The device that initiated the waiting call plays a call waiting ringback tone to the calling party after a 182 response is received.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The device's Call Progress Tones (CPT) file must include a Call</li> </ul>

Parameter	Description
	<p>Waiting ringback tone (caller side) and a call waiting tone (called side, FXS only).</p> <ul style="list-style-type: none"> <li>FXS interfaces: The EnableHold parameter must be enabled on both the calling and the called side.</li> <li>Analog interfaces: You can use the table parameter CallWaitingPerPort to enable Call Waiting per port.</li> <li>Analog interfaces: For information on the Call Waiting feature, see Call Waiting on page 357.</li> </ul>
EMS: Send 180 For Call Waiting <b>[Send180ForCallWaiting]</b>	<p>Determines the SIP response code for indicating Call Waiting.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Use 182 Queued response to indicate call waiting.</li> <li><b>[1]</b> = Use 180 Ringing response to indicate call waiting.</li> </ul>
Call Waiting Table	
<p>Web: Call Waiting Table EMS: SIP Endpoints &gt; Call Waiting CLI: configure voip &gt; gw analoggw call-waiting <b>[CallWaitingPerPort]</b></p>	<p>This table parameter configures call waiting per FXS port. The format of this parameter is as follows:</p> <p><b>[CallWaitingPerPort]</b>  FORMAT CallWaitingPerPort_Index = CallWaitingPerPort_IsEnabled, CallWaitingPerPort_Module, CallWaitingPerPort_Port;  <b>[CallWaitingPerPort]</b></p> <p>For example:  CallWaitingPerPort 0 = 0,1,1; (call waiting disabled for Port 1 of Module 1)  CallWaitingPerPort 1 = 1,1,2; (call waiting enabled for Port 2 of Module 1)</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to FXS ports.</li> <li>For a detailed description of this table, see Configuring Call Waiting on page 402.</li> </ul>
<p>Web: Number of Call Waiting Indications EMS: Call Waiting Number of Indications CLI: nb-of-cw-ind <b>[NumberOfWaitingIndications]</b></p>	<p>Defines the number of call waiting indications that are played to the called telephone that is connected to the device for Call Waiting.</p> <p>The valid range is 1 to 100 indications. The default is 2.</p> <p><b>Note:</b> This parameter is applicable only to FXS ports.</p>
<p>Web: Time Between Call Waiting Indications EMS: Call Waiting Time Between Indications CLI: time-between-cw <b>[TimeBetweenWaitingIndications]</b></p>	<p>Defines the time (in seconds) between consecutive call waiting indications for call waiting.</p> <p>The valid range is 1 to 100. The default is 10.</p> <p><b>Note:</b> This parameter is applicable only to FXS ports.</p>
<p>Web/EMS: Time Before Waiting Indications CLI: time-b4-cw-ind <b>[TimeBeforeWaitingIndications]</b></p>	<p>Defines the interval (in seconds) before a call waiting indication is played to the port that is currently in a call.</p> <p>The valid range is 0 to 100. The default time is 0 seconds.</p> <p><b>Note:</b> This parameter is applicable only to FXS ports.</p>
<p>Web/EMS: Waiting Beep Duration CLI: waiting-beep-dur <b>[WaitingBeepDuration]</b></p>	<p>Defines the duration (in msec) of call waiting indications that are played to the port that is receiving the call.</p> <p>The valid range is 100 to 65535. The default is 300.</p> <p><b>Note:</b> This parameter is applicable only to FXS ports.</p>

Parameter	Description
EMS: First Call Waiting Tone ID <b>[FirstCallWaitingToneID]</b>	<p>Defines the index of the first Call Waiting Tone in the CPT file. This feature enables the called party to distinguish between different call origins (e.g., external versus internal calls).</p> <p>There are three ways to use the distinctive call waiting tones:</p> <ul style="list-style-type: none"> <li>Playing the call waiting tone according to the SIP Alert-Info header in the received 180 Ringing SIP response. The value of the Alert-Info header is added to the value of the FirstCallWaitingToneID parameter.</li> <li>Playing the call waiting tone according to PriorityIndex in the ToneIndex table parameter.</li> <li>Playing the call waiting tone according to the parameter "CallWaitingTone#" of a SIP INFO message.</li> </ul> <p>The device plays the tone received in the 'play tone CallWaitingTone#' parameter of an INFO message plus the value of this parameter minus 1.</p> <p>The valid range is -1 to 1,000. The default is -1 (i.e., not used).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to analog interfaces.</li> <li>It is assumed that all Call Waiting Tones are defined in sequence in the CPT file.</li> <li>SIP Alert-Info header examples: <ul style="list-style-type: none"> <li>✓ Alert-Info:&lt;Bellcore-dr2&gt;</li> <li>✓ Alert-Info:&lt;http://.../Bellcore-dr2&gt; (where "dr2" defines call waiting tone #2)</li> </ul> </li> <li>The SIP INFO message is according to Broadsoft's application server definition. Below is an example of such an INFO message:</li> </ul> <pre>INFO sip:06@192.168.13.2:5060 SIP/2.0 Via:SIP/2.0/UDP 192.168.13.40:5060;branch=z9hG4bK040066422630 From: &lt;sip:4505656002@192.168.13.40:5060&gt;;tag=1455352915 To: &lt;sip:06@192.168.13.2:5060&gt; Call-ID:0010-0008@192.168.13.2 CSeq:342168303 INFO Content-Length:28 Content-Type:application/broadsoft play tone CallWaitingTone1</pre>

### 59.11.5.3 Call Forwarding Parameters

The call forwarding parameters are described in the table below.

**Call Forwarding Parameters**

Parameter	Description
Web: Enable Call Forward CLI: call-forward <b>[EnableForward]</b>	<p>Enables the Call Forwarding feature.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (Default)</li> </ul> <p>For FXS interfaces, the Call Forward table (FwdInfo parameter) must be defined to use the Call Forward service. The device uses SIP REFER messages for call forwarding.</p>



Parameter	Description
	<b>Note:</b> To use this service, the devices at both ends must support this option.
Call Forwarding Table	
Web: Call Forwarding Table EMS: Analog Gateway Provisioning > Tab: Call Forward CLI: configure voip > gw analoggw call-forward <b>[FwdInfo]</b>	<p>This table parameter configures call forwarding of IP-to-Tel calls (using SIP 302 response) to other device ports or an IP destination, based on the device's port to which the call was originally routed.</p> <p>The format of this parameter is as follows:</p> <p><b>[FwdInfo]</b>  FORMAT FwdInfo_Index = FwdInfo_Type, FwdInfo_Destination, FwdInfo_NoReplyTime, FwdInfo_Module, FwdInfo_Port;  <b>[FwdInfo]</b></p> <p>Where,</p> <ul style="list-style-type: none"> <li>Module = Module number, where 1 denotes the module in Slot 1.</li> <li>Port = Port number, where 1 denotes Port 1 of a module.</li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>Below configuration forwards calls originally destined to Port 1 of Module 1 to "1001" upon On Busy:  FwdInfo 0 = 1,1001,30,1,1;</li> <li>Below configuration forwards calls originally destined to Port 2 of Module 1 to an IP address upon On Busy:  FwdInfo 1 = 1,2003@10.5.1.1,30,1,2;</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The indexing of this parameter starts at 0.</li> <li>For a detailed description of this table, see Configuring Call Forward on page 399.</li> </ul>
Call Forward Reminder Ring Parameters <b>Notes:</b> <ul style="list-style-type: none"> <li>These parameters are applicable only to FXS interfaces.</li> <li>For a description of this feature, see Call Forward Reminder Ring on page 355.</li> </ul>	
Web/EMS: Enable NRT Subscription CLI: nrt-subscription <b>[EnableNRTSubscription]</b>	Enables endpoint subscription for Ring reminder event notification feature. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Web: AS Subscribe IPGroupID CLI: as-subs-ipgroupid <b>[ASSubscribeIPGroupID]</b>	Defines the IP Group ID that contains the Application server for Subscription. The valid value range is 1 to 8. The default is -1 (i.e., not configured).
Web: NRT Retry Subscription Time EMS: NRT Subscription Retry Time <b>[NRTSubscribeRetryTime]</b>	Defines the Retry period (in seconds) for Dialog subscription if a previous request failed. The valid value range is 10 to 7200. The default is 120.
Web/EMS: Call Forward Ring Tone ID CLI: cfe-ring-tone-id <b>[CallForwardRingToneID]</b>	Defines the ringing tone type played when call forward notification is accepted. The valid value range is 1 to 5. The default is 1.



### 59.11.5.4 Message Waiting Indication Parameters

The message waiting indication (MWI) parameters are described in the table below.

**MWI Parameters**

Parameter	Description
Web: Enable MWI EMS: MWI Enable CLI: enable-mwi <b>[EnableMWI]</b>	<p>Enables Message Waiting Indication (MWI).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to FXS interfaces.</li> <li>The device supports only the receipt of SIP MWI NOTIFY messages (the device doesn't generate these messages).</li> <li>For more information on MWI, see 'Message Waiting Indication' on page 358.</li> </ul>
Web/EMS: MWI Analog Lamp CLI: mwi-analog-lamp <b>[MWIAnalogLamp]</b>	<p>Enables the visual display of MWI.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> Enable = Enables visual MWI by supplying line voltage of approximately 100 VDC to activate the phone's lamp.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only for FXS interfaces.</li> <li>This parameter can also be configured in a Tel Profile.</li> </ul>
Web/EMS: MWI Display CLI: enable-mwi <b>[MWIDisplay]</b>	<p>Enables sending MWI information to the phone display.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) MWI information isn't sent to display.</li> <li><b>[1]</b> Enable = The device generates an MWI message (determined by the parameter CallerIDType), which is displayed on the MWI display.</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to FXS interfaces.</li> <li>This parameter can also be configured in a Tel Profile.</li> </ul>
Web: Subscribe to MWI EMS: Enable MWI Subscription CLI: subscribe-to-mwi <b>[EnableMWISubscription]</b>	<p>Enables subscription to an MWI server.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No (default)</li> <li><b>[1]</b> Yes</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To configure the MWI server address, use the MWIServerIP parameter.</li> <li>To configure whether the device subscribes per endpoint or per the entire device, use the parameter SubscriptionMode.</li> </ul>
Web: MWI Server IP Address EMS: MWI Server IP CLI: mwi-srvr-ip-addr <b>[MWIServerIP]</b>	<p>Defines the MWI server's IP address. If provided, the device subscribes to this IP address. The MWI server address can be configured as a numerical IP address or as a domain name. If not configured, the Proxy IP address is used instead.</p>
Web/EMS: MWI Server Transport Type CLI: mwi-srvr-transp-type <b>[MWIServerTransportT]</b>	<p>Determines the transport layer used for outgoing SIP dialogs initiated by the device to the MWI server.</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured (default)</li> <li><b>[0]</b> UDP</li> <li><b>[1]</b> TCP</li> </ul>

Parameter	Description
<b>ype]</b>	<ul style="list-style-type: none"> <li><b>[2]</b> TLS</li> </ul> <p><b>Note:</b> When set to 'Not Configured', the value of the parameter SIPTransportType is used.</p>
Web: MWI Subscribe Expiration Time EMS: MWI Expiration Time CLI: mwi-subs-expr-time <b>[MWIExpirationTime]</b>	Defines the MWI subscription expiration time in seconds. The default is 7200 seconds. The range is 10 to 2,000,000.
Web: MWI Subscribe Retry Time EMS: Subscribe Retry Time CLI: mwi-subs-rtry-time <b>[SubscribeRetryTime]</b>	Defines the subscription retry time (in seconds) after last subscription failure. The default is 120 seconds. The range is 10 to 2,000,000.
Web: Subscription Mode CLI: subscription-mode <b>[SubscriptionMode]</b>	Determines the method the device uses to subscribe to an MWI server. <ul style="list-style-type: none"> <li><b>[0]</b> Per Endpoint = (Default) Each endpoint subscribes separately - typically used for FXS interfaces.</li> <li><b>[1]</b> Per Gateway = Single subscription for the entire device - typically used for FXO interfaces.</li> </ul>
EMS: ETSI VMWI Type One Standard CLI: etsi-vmwi-type-one-standard <b>[ETSIVMWITypeOneStandard]</b>	Determines the ETSI Visual Message Waiting Indication (VMWI) Type 1 sub-standard. <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) ETSI VMWI between rings</li> <li><b>[1]</b> = ETSI VMWI before ring DT_AS</li> <li><b>[2]</b> = ETSI VMWI before ring RP_AS</li> <li><b>[3]</b> = ETSI VMWI before ring LR_DT_AS</li> <li><b>[4]</b> = ETSI VMWI not ring related DT_AS</li> <li><b>[5]</b> = ETSI VMWI not ring related RP_AS</li> <li><b>[6]</b> = ETSI VMWI not ring related LR_DT_AS</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: Bellcore VMWI Type One Standard CLI: bellcore-vmwi-type-one-standard <b>[BellcoreVMWITypeOneStandard]</b>	Determines the Bellcore VMWI sub-standard. <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Between rings.</li> <li><b>[1]</b> = Not ring related.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>

### 59.11.5.5 Call Hold Parameters

The call hold parameters are described in the table below.

**Call Hold Parameters**

Parameter	Description
Web/EMS: Enable Hold CLI: hold <b>[EnableHold]</b>	<p>For digital interfaces: Enables interworking of the Hold/Retrieve supplementary service from PRI to SIP.</p> <p>For analog interfaces: Enables the Call Hold feature that allows users, connected to the device, to place a call on hold (or remove from hold). This is done using the phone's Hook Flash button. On receiving a hold request, the remote party is placed on hold and hears the hold tone.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable</li> <li>▪ <b>[1]</b> Enable (default)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For digital interfaces: To support interworking of the Hold/Retrieve supplementary service from SIP to ISDN (for QSIG and Euro ISDN), set the parameter EnableHold2ISDN to 1.</li> <li>▪ For analog interfaces: To use this service, the devices at both ends must support this option.</li> <li>▪ This parameter can also be configured in an IP Profile.</li> </ul>
Web/EMS: Hold Format CLI: hold-format <b>[HoldFormat]</b>	<p>Determines the format of the SDP in the sent Re-INVITE hold request.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> 0.0.0.0 = (Default) The SDP "c=" field contains the IP address "0.0.0.0" and the "a=inactive" attribute.</li> <li>▪ <b>[1]</b> Send Only = The SDP "c=" field contains the device's IP address and the "a=sendonly" attribute.</li> <li>▪ <b>[2]</b> x.y.z.t = The SDP "c=" field contains the device's IP address and the "a=inactive" attribute.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The device does not send any RTP packets when it is in hold state.</li> <li>▪ For digital interfaces: This parameter is applicable only to QSIG and Euro ISDN protocols.</li> </ul>
Web/EMS:Held Timeout CLI: held-timeout <b>[HeldTimeout]</b>	<p>Defines the time interval that the device allows for a call to remain on hold. If a Resume (un-hold Re-INVITE) message is received before the timer expires, the call is renewed. If this timer expires, the call is released (terminated).</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> = (Default) The call is placed on hold indefinitely until the initiator of the on hold retrieves the call again.</li> <li>▪ <b>[0 - 2400]</b> = Time to wait (in seconds) after which the call is released.</li> </ul>
Web: Call Hold Reminder Ring Timeout EMS: CHRRTIMEOUT CLI: call-hold-remnd-rng <b>[CHRRTIMEOUT]</b>	<p>Defines the duration (in seconds) that the Call Hold Reminder Ring is played. If a user hangs up while a call is still on hold or there is a call waiting, then the FXS interface immediately rings the extension for the duration specified by this parameter. If the user off-hooks the phone, the call becomes active.</p> <p>The valid range is 0 to 600. The default is 30.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to FXS interfaces.</li> <li>▪ This Reminder Ring feature can be disabled using the DisableReminderRing parameter.</li> </ul>
CLI: dis-reminder-ring	Disables the reminder ring, which notifies the FXS user of a call on hold

Parameter	Description
<b>[DisableReminderRing]</b>	<p>or a waiting call when the phone is returned to on-hook position.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) The reminder ring feature is active. In other words, if a call is on hold or there is a call waiting and the phone is changed from offhook to onhook, the phone rings (for a duration defined by the CHRRTimeout parameter) to "remind" you of the call hold or call waiting.</li> <li><b>[1]</b> = Disables the reminder ring. If a call is on hold or there is a call waiting and the phone is changed from offhook to onhook, the call is released (and the device sends a SIP BYE to the IP).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to FXS interfaces.</li> <li>This parameter is typically used for MLPP, allowing preemption to clear held calls.</li> </ul>
CLI: dtmf-during-hold <b>[PlayDTMFduringHold]</b>	<p>Determines whether the device sends DTMF signals (or DTMF SIP INFO message) when a call is on hold.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disable.</li> <li><b>[1]</b> = Enable - If the call is on hold, the device stops playing the Held tone (if it is played) and sends DTMF: <ul style="list-style-type: none"> <li>✓ To Tel side: plays DTMF digits according to the received SIP INFO message(s). (The stopped held tone is not played again.)</li> <li>✓ To IP side: sends DTMF SIP INFO messages to an IP destination if it detects DTMF digits from the Tel side.</li> </ul> </li> </ul>

### 59.11.5.6 Call Transfer Parameters

The call transfer parameters are described in the table below.

**Call Transfer Parameters**

Parameter	Description
Web/EMS: Enable Transfer CLI: enable-transfer <b>[EnableTransfer]</b>	<p>Enables the Call Transfer feature.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable = (Default) The device responds to a REFER message with the Referred-To header to initiate a call transfer. For analog interfaces: If the transfer service is enabled, the user can activate Transfer using hook-flash signaling. If this service is enabled, the remote party performs the call transfer.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To use call transfer, the devices at both ends must support this option.</li> <li>To use call transfer, set the parameter EnableHold to 1.</li> </ul>
Web: Transfer Prefix EMS: Logical Prefix For Transferred Call CLI: transfer-prefix <b>[xferPrefix]</b>	<p>Defines the string that is added as a prefix to the transferred/forwarded called number when the REFER/3xx message is received.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The number manipulation rules apply to the user part of the Refer-To and/or Contact URI before it is sent in the INVITE message.</li> <li>This parameter can be used to apply different manipulation rules to differentiate transferred/forwarded (only for analog interfaces) number from the originally dialed number.</li> </ul>
Web: Transfer Prefix IP 2	Defines the prefix that is added to the destination number received in the

Parameter	Description
Tel CLI: xfer-prefix-ip2tel <b>[XferPrefixIP2Tel]</b>	<p>SIP Refer-To header (for IP-to-Tel calls). This parameter is applicable to FXO/CAS blind transfer modes, i.e., LineTransferMode = 1, 2 or 3, and TrunkTransferMode = 1 or 3 (for CAS).</p> <p>The valid range is a string of up to 9 characters. The default is an empty string.</p> <p><b>Note:</b> This parameter is also applicable to ISDN Blind Transfer, according to AT&amp;T Toll Free Transfer Connect Service (TR 50075) "Courtesy Transfer-Human-No Data". To support this transfer mode, you need to configure the parameter XferPrefixIP2Tel to "*" and the parameter TrunkTransferMode to 5.</p>
Web/EMS: Enable Semi-Attended Transfer CLI: semi-att-transfer <b>[EnableSemiAttendedTransfer]</b>	<p>Determines the device behavior when Transfer is initiated while in Alerting state.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) Send REFER with the Replaces header.</li> <li>▪ <b>[1]</b> Enable = Send CANCEL, and after a 487 response is received, send REFER without the Replaces header.</li> </ul>
Web: Blind EMS: Blind Transfer CLI: blind-transfer <b>[KeyBlindTransfer]</b>	<p>Defines the keypad sequence to activate blind transfer for established Tel-to-IP calls. The Tel user can perform blind transfer by dialing the KeyBlindTransfer digits, followed by a transferee destination number.</p> <p>After the KeyBlindTransfer DTMF digits sequence is dialed, the current call is put on hold (using a Re-INVITE message), a dial tone is played to the channel, and then the phone number collection starts.</p> <p>After the destination phone number is collected, it is sent to the transferee in a SIP REFER request in a Refer-To header. The call is then terminated and a confirmation tone is played to the channel. If the phone number collection fails due to a mismatch, a reorder tone is played to the channel.</p> <p><b>Note:</b> For FXS/FXO interfaces, it is possible to configure whether the KeyBlindTransfer code is added as a prefix to the dialed destination number, by using the parameter KeyBlindTransferAddPrefix.</p>
EMS: Blind Transfer Add Prefix CLI: blind-xfer-add-prefix <b>[KeyBlindTransferAddPrefix]</b>	<p>Determines whether the device adds the Blind Transfer code (defined by the KeyBlindTransfer parameter) to the dialed destination number.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> This parameter is applicable only to FXO and FXS interfaces.</p>
EMS: Blind Transfer Disconnect Timeout CLI: blind-xfer-disc-tmo <b>[BlindTransferDisconnectTimeout]</b>	<p>Defines the duration (in milliseconds) for which the device waits for a disconnection from the Tel side after the Blind Transfer Code (KeyBlindTransfer) has been identified. When this timer expires, a SIP REFER message is sent toward the IP side. If this parameter is set to 0, the REFER message is immediately sent.</p> <p>The valid value range is 0 to 1,000,000. The default is 0.</p>
Web: QSIG Path Replacement Mode CLI: qsig-path-replacement-md <b>[QSIGPathReplacementMode]</b>	<p>Enables QSIG transfer for IP-to-Tel and Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> IP2QSIGTransfer = (Default) Enables IP-to-QSIG transfer.</li> <li>▪ <b>[1]</b> QSIG2IPTransfer = Enables QSIG-to-IP transfer.</li> </ul>

Parameter	Description
CLI: replace-tel2ip-calnum-to <b>[ReplaceTel2IPCallingNumTimeout]</b>	<p>Defines the maximum duration (timeout) to wait between call Setup and Facility with Redirecting Number for replacing the calling number (for Tel-to-IP calls).</p> <p>The valid value range is 0 to 10,000 msec. The default is 0.</p> <p>The interworking of the received Setup message to a SIP INVITE is suspended when this parameter is set to any value greater than 0. This means that the redirecting number in the Setup message is not checked. When a subsequent Facility with Call Transfer Complete/Update is received with a non-empty Redirection Number, the Calling Number is replaced with the received redirect number in the sent INVITE message. If the timeout expires, the device sends the INVITE without changing the calling number.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The suspension of the INVITE message occurs for all calls.</li> <li>▪ This parameter is applicable to QSIG.</li> </ul>
Web: Call Transfer using re-INVITES CLI: enable-call-transfer-using-reinvites <b>[EnableCallTransferUsingReinvites]</b>	<p>Enables call transfer using re-INVITES.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) Call transfer is done using REFER messages.</li> <li>▪ <b>[1]</b> Enable = Call transfer is done by sending re-INVITE messages (instead of REFER).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The device uses two DSP channels per transferred call. Thus, to use this feature, you also need to configure the maximum number of available DSP channels, using the MediaChannels parameter.</li> <li>▪ This parameter is applicable only to FXS interfaces.</li> </ul>
Web: IP2IP Transfer Mode CLI: ip2ip-transfer-mode <b>[IP2IPTransfermode]</b>	<p>Determines the interworking of incoming mid-call SIP REFER messages to outgoing REFER messages, for calls pertaining to the IP-to-IP application.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) Upon receipt of a REFER message, the device sends an INVITE to the refer-to destination with or without the Replaces header.</li> <li>▪ <b>[1]</b> Enable = Upon receipt of a REFER message, the device forwards the REFER message and all relevant SIP messages from and to the transferor, to the target destination during call transfer. For consultation call transfer, the REFER message contains a 'replaces' parameter in the Refer-To header. In this case, the outgoing REFER also contains a 'replaces' parameter in the Refer-To header.</li> </ul> <p><b>Note:</b> This parameter is applicable to blind and consultation call transfers.</p>

### 59.11.5.7 Three-Way Conferencing Parameters

The three-way conferencing parameters are described in the table below.

**Three-Way Conferencing Parameters**

Parameter	Description
Web: Enable 3-Way Conference EMS: Enable 3 Way CLI: enable-3w-conf <b>[Enable3WayConference]</b>	Enables the 3-Way Conference feature. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: Three Way Conference Mode EMS: 3 Way Mode CLI: 3w-conf-mode <b>[3WayConferenceMode]</b>	Determines the mode of operation when the 3-Way Conference feature is used. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> AudioCodes Media Server = (Default) The Conference-initiating INVITE (sent by the device) uses the ConferenceID concatenated with a unique identifier as the Request-URI. This same Request-URI is set as the Refer-To header value in the REFER messages that are sent to the two remote parties. This conference mode is used when operating with AudioCodes IPMedia conferencing server.</li> <li>▪ <b>[1]</b> Non-AudioCodes Media Server = The Conference-initiating INVITE (sent by the device) uses only the ConferenceID as the Request-URI. The conference server sets the Contact header of the 200 OK response to the actual unique identifier (Conference URI) to be used by the participants. This Conference URI is then included (by the device) in the Refer-To header value in the REFER messages sent by the device to the remote parties. The remote parties join the conference by sending INVITE messages to the conference using this conference URI.</li> <li>▪ <b>[2]</b> On Board = On-board, three-way conference. The conference is established on the device without the need of an external Conference server. You can limit the number of simultaneous, on-board 3-way conference calls, by using the MaxInBoardConferenceCalls parameter.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to FXS and BRI interfaces.</li> <li>▪ Three-way conferencing using an external conference server is supported only by FXS interfaces.</li> <li>▪ When using an external conference server (options <b>[0]</b> or <b>[1]</b>), a conference call with up to six participants can be established.</li> </ul>
Web: Max 3 Way Conference EMS: Max In Board Calls <b>[MaxInBoardConferenceCalls]</b>	Defines the maximum number of simultaneous, on-board three-way conference calls. The valid range is 0 to 5. The default is 2. <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ For enabling on-board, three-way conferencing, use the 3WayConferenceMode parameter.</li> <li>▪ This parameter is applicable only to FXS and BRI interfaces.</li> </ul>



Parameter	Description
Web: Establish Conference Code EMS: Establish Code CLI: estb-conf-code <b>[ConferenceCode]</b>	<p>Defines the DTMF digit pattern, which upon detection generates the conference call when three-way conferencing is enabled (Enable3WayConference is set to 1).</p> <p>The valid range is a 25-character string. The default is "!" (Hook-Flash).</p> <p><b>Note:</b> If the FlashKeysSequenceStyle parameter is set to 1 or 2, the setting of the ConferenceCode parameter is overridden.</p>
Web/EMS: Conference ID CLI: conf-id <b>[ConferenceID]</b>	<p>Defines the Conference Identification string.</p> <p>The valid value is a string of up to 16 characters. The default is "conf".</p> <p>The device uses this identifier in the conference-initiating INVITE that is sent to the media server when the Enable3WayConference parameter is set to 1.</p>
Web: Use Different RTP port After Hold CLI: use-different-rtp-port-after-hold <b>[UseDifferentRTPportAfterHold]</b>	<p>Enables the use of different RTP ports for the two calls involved in a three-way conference call made by the FXS endpoint in the initial outgoing INVITE requests.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = First and second calls use the same RTP port in the initial outgoing INVITE request. If a three-way conference is then made, the device sends a re-INVITE to the held call to retrieve it and to change the RTP port to a different port number.</li> </ul> <p>For example: The first call is made on port 6000 and placed on hold. The second call is made, also on port 6000. The device sends a re-INVITE to the held call to retrieve it and changes the port to 6010.</p> <ul style="list-style-type: none"> <li><b>[1]</b> Enable = First and second calls use different RTP ports in the initial outgoing INVITE request. If a three-way conference is then made, the device sends a re-INVITE to the held call to retrieve it, without changing the port of the held call.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>When this feature is enabled and only one RTP port is available, only one call can be made by the FXS endpoint, as there is no free RTP port for a second call.</li> <li>When this feature is enabled and you are using the Call Forking feature, every forked call is sent with a different RTP port. As the device can fork a call to up to 10 destinations, the device requires at least 10 free RTP ports.</li> <li>This parameter is applicable only to FXS interfaces.</li> </ul>

#### 59.11.5.8 MLPP and Emergency Call Parameters

The Multilevel Precedence and Preemption (MLPP) and emergency E911 call parameters are described in the table below.

**MLPP and Emergency E911 Call Parameters**

Parameter	Description
Web/EMS: Call Priority Mode CLI: call-prio-mode <b>[CallPriorityMode]</b>	<p>Enables priority call handling for all calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> MLPP = MLPP Priority Call handling is enabled. MLPP prioritizes call handling whereby the relative importance of various kinds of communications is strictly defined, allowing higher precedence communication at the expense of lower precedence communications. Higher priority calls override less priority calls when, for example, congestion occurs in a network.</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[2]</b> Emergency = Preemption of IP-to-Tel E911 emergency calls. If the device receives an E911 call and there are unavailable channels to receive the call, the device terminates one of the channel calls and sends the E911 call to that channel. The preemption is done only on a channel pertaining to the same Trunk Group for which the E911 call was initially destined and if the channel select mode (configured by the ChannelSelectMode parameter) is set to other than "By Dest Number" (0). The preemption is done only if the incoming IP-to-Tel call is identified as an emergency call. The device identifies emergency calls by one of the following: <ul style="list-style-type: none"> <li>✓ The destination number of the IP call matches one of the numbers defined by the EmergencyNumbers parameter. (For E911, you must define this parameter with the value "911".)</li> <li>✓ The incoming SIP INVITE message contains the "emergency" value in the Priority header.</li> </ul> </li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable to FXS/FXO, CAS, and ISDN.</li> <li>▪ For FXO interfaces, the preemption is done only on existing IP-to-Tel calls. In other words, if all the current FXO channels are busy with calls that were initiated by the FXO (i.e., Tel-to-IP calls), new incoming emergency IP-to-Tel calls are dropped.</li> <li>▪ MLPP and Emergency services can also be configured in a Tel Profile.</li> <li>▪ For more information, see 'Pre-empting Existing Call for E911 IP-to-Tel Call' on page 369.</li> </ul>
<b>Emergency E911 Parameters</b>	
<b>[E911Gateway]</b>	<p>Enables Enhanced 9-1-1(E9-1-1) support for ELIN handling in Microsoft Lync Server 2010 environment.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> <li>▪ <b>[2]</b> = Location-based manipulations</li> </ul>
<b>[E911CallbackTimeout]</b>	<p>Defines the maximum interval within which the PSAP can use the ELIN to call back the E9-1-1 caller. This interval starts from when the initial call established with the PSAP is terminated.</p> <p>The valid range is 1 to 60 (minutes). The default is 30.</p>
Web: Emergency Special Release Cause CLI: emrg-spcl-rel-cse <b>[EmergencySpecialReleaseCause]</b>	<p>Enables the device to send a SIP 503 "Service Unavailable" response if an emergency call cannot be established (i.e., rejected). This can occur, for example, due to the PSTN (for example, the destination is busy or not found) or ELIN Gateway (for example, lack of resources or an internal error).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul>
EMS: Enable 911 PSAP <b>[Enable911PSAP]</b>	<p>Enables the support for the E911 DID protocol, according to the Bellcore GR-350-CORE standard. This protocol defines signaling between E911 Tandem Switches and the PSAP, using analog loop-start lines. The FXO device can be installed instead of an E911 switch, connected directly to PSAP DID loop-start lines.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul>

Parameter	Description
	<b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to FXO interfaces.</li> <li>This parameter can also be configured in a Tel Profile.</li> </ul>
Web/EMS: Emergency Numbers CLI: emerg-nbs <b>[EmergencyNumbers]</b>	<p>Defines a list of “emergency” numbers.</p> <p>For FXS: When one of these numbers is dialed, the outgoing INVITE message includes the SIP Priority and Resource-Priority headers. If the user places the phone on-hook, the call is not disconnected. Instead, a Hold Re-INVITE request is sent to the remote party. Only if the remote party disconnects the call (i.e., a BYE is received) or a timer expires (set by the EmergencyRegretTimeout parameter) is the call terminated.</p> <p>For FXO, CAS, and ISDN: These emergency numbers are used for the preemption of E911 IP-to-Tel calls when there are unavailable or busy channels. In this scenario, the device terminates one of the busy channels and sends the emergency call to this channel. This feature is enabled by setting the CallPriorityMode parameter to 2 (“Emergency”). For a description of this feature, see 'Pre-empting Existing Call for E911 IP-to-Tel Call' on page <a href="#">369</a>.</p> <p>The list can include up to four different numbers, where each number can be up to four digits long.</p> <p>Example: EmergencyNumbers = ‘100’, ‘911’, ‘112’</p>
Web: Emergency Calls Regret Timeout EMS: Emergency Regret Timeout CLI: emerg-calls-regrt-t-out <b>[EmergencyRegretTimeout]</b>	<p>Defines the time (in minutes) that the device waits before tearing-down an emergency call (defined by the parameter EmergencyNumbers). Until this time expires, an emergency call can only be disconnected by the remote party, typically, by a Public Safety Answering Point (PSAP). The valid range is 1 to 30. The default is 10.</p> <p><b>Note:</b> This parameter is applicable only to FXS interfaces.</p>
<b>Multilevel Precedence and Preemption (MLPP) Parameters</b>	
Web: MLPP Default Namespace EMS: Default Namespace CLI: mlpp-dflt-namespace <b>[MLPPDefaultNamespace]</b>	<p>Determines the namespace used for MLPP calls received from the ISDN side without a Precedence IE and destined for an Application server. This value is used in the Resource-Priority header of the outgoing SIP INVITE request.</p> <ul style="list-style-type: none"> <li><b>[1]</b> DSN (default)</li> <li><b>[2]</b> DOD</li> <li><b>[3]</b> DRSN</li> <li><b>[5]</b> UC</li> <li><b>[7]</b> CUC</li> </ul> <p><b>Note:</b> If the ISDN message contains a Precedence IE, the device automatically interworks the “network identity” digits in the IE to the network domain subfield in the Resource-Priority header. For more information, see Multilevel Precedence and Preemption on page <a href="#">382</a>.</p>
<b>[ResourcePriorityNetworkDomains]</b>	<p>Defines up to 32 user-defined MLPP network domain names (namespaces). This value is used in the AS-SIP Resource-Priority header of the outgoing SIP INVITE request. This parameter is used in combination with the MLPPDefaultNamespace parameter, where you need to enter the table row index as its value.</p> <p>This parameter is also used for mapping the Resource-Priority field value of the SIP Resource-Priority header to the ISDN PRI Precedence Level IE. The mapping is configured by the field, EnableIp2TelInterworking:</p>

Parameter	Description
	<ul style="list-style-type: none"> <li>Disabled: The network-domain field in the Resource-Priority header is set to "0 1 0 0" (i.e., "routine") in the Precedence Level field.</li> <li>Enabled: The network-domain field in the Resource-Priority header is set in the Precedence Level field according to Table 5.3.2.12-4 (Mapping of RPH r-priority Field to PRI Precedence Level Value).</li> </ul> <p>The domain name can be a string of up to 10 characters.</p> <p>The format of this table ini file parameter is as follows:          FORMAT ResourcePriorityNetworkDomains_Index =          ResourcePriorityNetworkDomains_Name,          ResourcePriorityNetworkDomains_EnableIp2TelInterworking;          ResourcePriorityNetworkDomains 1 = dsn, 0;          ResourcePriorityNetworkDomains 2 = dod, 0;          ResourcePriorityNetworkDomains 3 = drsn, 0;          ResourcePriorityNetworkDomains 5 = uc, 1;          ResourcePriorityNetworkDomains 7 = cuc, 0;          [ \ResourcePriorityNetworkDomains ]</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Indices 1, 2, 3, 5, and 7 cannot be modified and are defined for DSN, DOD, DRSN, UC, and CUC, respectively.</li> <li>If the MLPPDefaultNamespace parameter is set to -1, interworking from PSTN NI digits is done automatically.</li> </ul>
Web/EMS: Default Call Priority CLI: dflt-call-prio [SIPDefaultCallPriority]	<p>Determines the default call priority for MLPP calls.</p> <ul style="list-style-type: none"> <li>[0] 0 = (Default) ROUTINE</li> <li>[2] 2 = PRIORITY</li> <li>[4] 4 = IMMEDIATE</li> <li>[6] 6 = FLASH</li> <li>[8] 8 = FLASH-OVERRIDE</li> <li>[9] 9 = FLASH-OVERRIDE-OVERRIDE</li> </ul> <p>If the incoming SIP INVITE request doesn't contain a valid priority value in the SIP Resource-Priority header, the default is used in the Precedence IE (after translation to the relevant ISDN Precedence value) of the outgoing PRI Setup message.</p> <p>If the incoming PRI Setup message doesn't contain a valid Precedence Level value, the default is used in the Resource-Priority header of the outgoing SIP INVITE request. In this scenario, the character string is sent without translation to a numerical value.</p>
Web: MLPP DiffServ EMS: Diff Serv CLI: mlpp-diffserv [MLPPDiffserv]	<p>Defines the DiffServ value (differentiated services code point/DSCP) used in IP packets containing SIP messages that are related to MLPP calls. This parameter defines DiffServ for incoming and outgoing MLPP calls with the Resource-Priority header.</p> <p>The valid range is 0 to 63. The default is 50.</p>
Web/EMS: Preemption Tone Duration CLI: preemp-tone-dur [PreemptionToneDuration]	<p>Defines the duration (in seconds) in which the device plays a preemption tone to the Tel and IP sides if a call is preempted.</p> <p>The valid range is 0 to 60. The default is 3.</p> <p><b>Note:</b> If set to 0, no preemption tone is played.</p>
Web: MLPP Normalized Service Domain EMS: Normalized Service Domain	<p>Defines the MLPP normalized service domain string. If the device receives an MLPP ISDN incoming call, it uses the parameter (if different from 'FFFFFF') as a Service domain in the SIP Resource-Priority header in outgoing INVITE messages. If the parameter is configured to</p>

Parameter	Description
CLI: mlpp-norm-ser-dmn <b>[MLPPNormalizedServiceDomain]</b>	<p>'FFFFFF', the Resource-Priority header is set to the MLPP Service Domain obtained from the Precedence IE.</p> <p>The valid value is 6 hexadecimal digits. The default is '000000'.</p> <p><b>Note:</b> This parameter is applicable only to the MLPP NI-2 ISDN variant with CallPriorityMode set to 1.</p>
CLI: mlpp-nwrk-id <b>[MLPPNetworkIdentifier]</b>	<p>Defines the MLPP network identifier (i.e., International prefix or Telephone Country Code/TCC) for IP-to-ISDN calls, according to the UCR 2008 and ITU Q.955 specifications.</p> <p>The valid range is 1 to 999. The default is 1 (i.e., USA).</p> <p>The MLPP network identifier is sent in the Facility IE of the ISDN Setup message. For example:</p> <ul style="list-style-type: none"> <li>MLPPNetworkIdentifier set to default (i.e., USA, 1): PlaceCall- MLPPNetworkID:0100 MlppServiceDomain:123abc, MlppPrecLevel:5 Fac(1c): 91 a1 15 02 01 05 02 01 19 30 0d 0a 01 05 0a 01 01 04 05 01 00 12 3a bc</li> <li>MLPPNetworkIdentifier set to 490: PlaceCall- MLPPNetworkID:9004 MlppServiceDomain:123abc, MlppPrecLevel:5 Fac(1c): 91 a1 15 02 01 0a 02 01 19 30 0d 0a 01 05 0a 01 01 04 05 90 04 12 3a bc</li> </ul>
Web: MLPP Default Service Domain EMS: Default Service Domain CLI: mlpp-dflt-srv-domain <b>[MLPPDefaultServiceDomain]</b>	<p>Defines the MLPP default service domain string. If the device receives a non-MLPP ISDN incoming call (without a Precedence IE), it uses the parameter (if different than "FFFFFF") as a Service domain in the SIP Resource-Priority header in outgoing (Tel-to-IP calls) INVITE messages. This parameter is used in conjunction with the parameter SIPDefaultCallPriority.</p> <p>If MLPPDefaultServiceDomain is set to 'FFFFFF', the device interworks the non-MLPP ISDN call to non-MLPP SIP call, and the outgoing INVITE does not contain the Resource-Priority header.</p> <p>The valid value is a 6 hexadecimal digits. The default is "000000".</p> <p><b>Note:</b> This parameter is applicable only to the MLPP NI-2 ISDN variant with CallPriorityMode set to 1.</p>
Web/EMS: Precedence Ringing Type CLI: precedence-ringing <b>[PrecedenceRingingType]</b>	<p>Defines the index of the Precedence Ringing tone in the Call Progress Tones (CPT) file. This tone is used when the parameter CallPriorityMode is set to 1 and a Precedence call is received from the IP side.</p> <p>The valid range is -1 to 16. The default is -1 (i.e., plays standard ringing tone).</p> <p><b>Note:</b> This parameter is applicable only to analog interfaces.</p>
EMS: E911 MLPP Behavior CLI: e911-mlpp-bhvr <b>[E911MLPPBehavior]</b>	<p>Defines the E911 (or Emergency Telecommunication Services/ETS) MLPP Preemption mode:</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Standard Mode - ETS calls have the highest priority and preempt any MLPP call.</li> <li><b>[1]</b> = Treat as routine mode - ETS calls are handled as routine calls.</li> </ul> <p><b>Note:</b> This parameter is applicable only to analog interfaces.</p>
CLI: resource-prio-req <b>[RPRequired]</b>	<p>Determines whether the SIP resource-priority tag is added in the SIP Require header of the INVITE message for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Excludes the SIP resource-priority tag from the SIP Require header.</li> </ul>

Parameter	Description														
	<ul style="list-style-type: none"> <li><b>[1]</b> Enable = (Default) Adds the SIP resource-priority tag in the SIP Require header.</li> </ul> <p><b>Note:</b> This parameter is applicable only to MLPP priority call handling (i.e., only when the CallPriorityMode parameter is set to 1).</p>														
<b>Multiple Differentiated Services Code Points (DSCP) per MLPP Call Priority Level (Precedence) Parameters</b> <p>The MLPP service allows placement of priority calls, where properly validated users can preempt (terminate) lower-priority phone calls with higher-priority calls. For each MLPP call priority level, the DSCP can be set to a value from 0 to 63. The Resource Priority value in the Resource-Priority SIP header can be one of the following:</p> <table> <thead> <tr> <th>MLPP Precedence Level</th><th>Precedence Level in Resource-Priority SIP Header</th></tr> </thead> <tbody> <tr> <td>0 (lowest)</td><td>routine</td></tr> <tr> <td>2</td><td>priority</td></tr> <tr> <td>4</td><td>immediate</td></tr> <tr> <td>6</td><td>flash</td></tr> <tr> <td>8</td><td>flash-override</td></tr> <tr> <td>9 (highest)</td><td>flash-override-override</td></tr> </tbody> </table>		MLPP Precedence Level	Precedence Level in Resource-Priority SIP Header	0 (lowest)	routine	2	priority	4	immediate	6	flash	8	flash-override	9 (highest)	flash-override-override
MLPP Precedence Level	Precedence Level in Resource-Priority SIP Header														
0 (lowest)	routine														
2	priority														
4	immediate														
6	flash														
8	flash-override														
9 (highest)	flash-override-override														
Web/EMS: RTP DSCP for MLPP Routine CLI: dscp-4-mlpp-rtn <b>[MLPPRoutineRTPDSCP]</b>	<p>Defines the RTP DSCP for MLPP Routine precedence call level. The valid range is -1 to 63. The default is -1.</p> <p><b>Note:</b> If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined in IP Profiles per call.</p>														
Web/EMS: RTP DSCP for MLPP Priority CLI: dscp-4-mlpp-prio <b>[MLPPPriorityRTPDSCP]</b>	<p>Defines the RTP DSCP for MLPP Priority precedence call level. The valid range is -1 to 63. The default is -1.</p> <p><b>Note:</b> If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined in IP Profiles per call.</p>														
Web/EMS: RTP DSCP for MLPP Immediate CLI: dscp-4-mlpp-immed <b>[MLPPImmediateRTPDSCP]</b>	<p>Defines the RTP DSCP for MLPP Immediate precedence call level. The valid range is -1 to 63. The default is -1.</p> <p><b>Note:</b> If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined in IP Profiles per call.</p>														
Web/EMS: RTP DSCP for MLPP Flash CLI: dscp-4-mlpp-flsh <b>[MLPPFlashRTPDSCP]</b>	<p>Defines the RTP DSCP for MLPP Flash precedence call level. The valid range is -1 to 63. The default is -1.</p> <p><b>Note:</b> If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined in IP Profiles per call.</p>														
Web/EMS: RTP DSCP for MLPP Flash Override CLI: dscp-4-mlpp-flsh-ov <b>[MLPPFlashOverRTPDSCP]</b>	<p>Defines the RTP DSCP for MLPP Flash-Override precedence call level. The valid range is -1 to 63. The default is -1.</p> <p><b>Note:</b> If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined in IP Profiles per call.</p>														
Web/EMS: RTP DSCP for MLPP Flash-Override-Override CLI: dscp-4-mlpp-flsh-ov-ov <b>[MLPPFlashOverOverRT]</b>	<p>Defines the RTP DSCP for MLPP Flash-Override-Override precedence call level. The valid range is -1 to 63. The default is -1.</p> <p><b>Note:</b> If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined in IP Profiles per call.</p>														

Parameter	Description
PDSCP]	

### 59.11.5.9 Call Cut-Through Parameters

The call cut-through parameters are described in the table below.

**Call Cut-Through Parameters**

Parameter	Description
Web: Enable Calls Cut Through EMS: Cut Through CLI: calls-cut-through <b>[CutThrough]</b>	<p>Enables FXS endpoints to receive incoming IP calls while the port is in off-hook state.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>If enabled, the FXS interface answers the call and 'cuts through' the voice channel if there is no other active call on the port, even if the port is in off-hook state.</p> <p>When the call is terminated (by the remote IP party), the device plays a reorder tone for a user-defined time (configured by the CutThroughTimeForReorderTone parameter) and is then ready to answer the next incoming call without on-hooking the phone.</p> <p>The waiting call is automatically answered by the device when the current call is terminated (configured by setting the parameter EnableCallWaiting to 1).</p> <p><b>Note:</b> This feature is applicable only to FXS interfaces.</p>
CLI: cut-through-anable <b>[DigitalCutThrough]</b>	<p>Enables PSTN CAS channels/endpoints to receive incoming IP calls even if the B-channels are in off-hook state.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disabled (default)</li> <li>▪ <b>[1]</b> Enabled</li> </ul> <p>When enabled, this feature operates as follows:</p> <ol style="list-style-type: none"> <li>1 A Tel-to-IP call is established (connected) by the device for a B-channel.</li> <li>2 The device receives a SIP BYE (i.e., IP side ends the call) and plays a reorder tone to the PSTN side for the duration set by the CutThroughTimeForReOrderTone parameter. The device releases the call towards the IP side (sends a SIP 200 OK).</li> <li>3 The PSTN side, for whatever reason, remains off-hook.</li> <li>4 If a new IP call is received for this B-channel after the reorder tone has ended, the device "cuts through" the channel and connects the call immediately (despite the B-channel being in physical off-hook state) without playing a ring tone. If an IP call is received while the reorder tone is played, the device rejects the call.</li> </ol> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If this parameter is disabled and the PSTN side remains in off-hook state after the IP call ends the call, the device releases the call after 60 seconds.</li> <li>▪ A special CAS table can be used to report call status events (Active/Idle) to the PSTN side during Cut Through mode.</li> <li>▪ This feature can also be configured in a Tel Profile and therefore, assigned to specific B-channels that use specific CAS tables.</li> </ul>



### 59.11.5.10 Automatic Dialing Parameters

The automatic dialing upon off-hook parameters are described in the table below.

**Automatic Dialing Parameters**

Parameter	Description
<b>Automatic Dialing Table</b>	
Web: Automatic Dialing Table EMS: Analog Gateway Provisioning > Automatic dialing CLI: configure voip/gw analoggw automatic-dialing <b>[TargetOfChannel]</b>	<p>This table parameter defines telephone numbers that are automatically dialed when a specific FXS or FXO port is off-hooked. The format of this parameter is as follows:</p> <p><b>[TargetOfChannel]</b>            FORMAT TargetOfChannel_Index = TargetOfChannel_Destination, TargetOfChannel_Type, TargetOfChannel_Module, TargetOfChannel_Port, TargetOfChannel_HotLineToneDuration;  <b>[TargetOfChannel]</b></p> <p>For example, the below configuration defines automatic dialing of phone number 911 when the phone connected to Port 1 of Module 1 is off-hooked for over 10 seconds:            TargetOfChannel 0 = 911, 1, 1, 1, 10;</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The first index of this table ini file parameter is 0.</li> <li>▪ TargetOfChannel_Module is the module number, where 1 denotes the module in Slot 1.</li> <li>▪ TargetOfChannel_Port is the port number, where 1 denotes Port 1 on the module.</li> <li>▪ This parameter is applicable only to FXS and FXO interfaces.</li> <li>▪ For a detailed description of this table, see 'Configuring Automatic Dialing' on page 396.</li> </ul>

### 59.11.5.11 Direct Inward Dialing Parameters

The Direct Inward Dialing (DID) parameters are described in the table below.

**DID Parameters**

Parameter	Description
Web/EMS: DID Wink CLI: did-wink-enbl <b>[EnableDIDWink]</b>	<p>Enables Direct Inward Dialing (DID) using Wink-Start signaling, typically used for signaling between an E-911 switch and the PSAP.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Single = The device can be used for connection to EIA/TIA-464B DID Loop Start lines. Both FXO (detection) and FXS (generation) are supported:               <ul style="list-style-type: none"> <li>✓ The FXO interface dials DTMF (or MF) digits upon detection of a Wink signal, instead of a dial tone.</li> <li>✓ The FXS interface generates a Wink signal upon detection of an off-hook state, instead of playing a dial tone.</li> </ul> </li> </ul> <p>Example: (Wink) KP I(I) xxx-xxxx ST (Off Hook)            Where:</p> <ul style="list-style-type: none"> <li>✓ I = one or two information digits</li> <li>✓ x = ANI</li> </ul>

Parameter	Description
	<p><b>Note:</b> The FXO interface generates such MF digits when the Enable911PSAP parameter is set to 1.</p> <ul style="list-style-type: none"> <li><b>[2] Double Wink = Double-wink signaling.</b> The FXS interface generates the first wink upon detection of an off-hook state in the line. The second wink is generated after a user-defined interval (configured by the TimeBetweenDIDWinks parameter), after which the DTMF/MF digits are collected by the device. Digits that arrive between the first and second wink are ignored as they contain the same number. Example: (Wink) KP 911 ST (Wink) KP I(l) xxx-xxxx ST (Off Hook)</li> <li><b>[3] Wink &amp; Polarity=</b> The FXS interface generates the first wink after it detects an off-hook state. A polarity change from normal to reversed is generated after a user-defined time (configured by the TimeBetweenDIDWinks parameter). DTMF/MF digits are collected only after this polarity change. Digits that arrive between the first wink and the polarity change are ignored as they always contain the same number. In this mode, the FXS interface does not generate a polarity change to normal if the Tel-to-IP call is answered by an IP party. Polarity reverts to normal when the call is released. Example: (Wink) KP 911 ST (Polarity) KP I(l) xxx-xxxx ST (Off Hook)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Options [2] and [3] are applicable only to FXS interfaces.</li> <li>The EnableReversalPolarity and PolarityReversalType parameters must be set to [1] for FXS interfaces.</li> <li>See also the Enable911PSAP parameter.</li> <li>This parameter can also be configured in a Tel Profile.</li> </ul>
<b>[TimeBetweenDIDWinks]</b>	<p>Defines the interval (in msec) for wink signaling:</p> <ul style="list-style-type: none"> <li>Double-wink signaling [2]: interval between the first and second wink.</li> <li>Wink and Polarity signaling [3]: interval between wink and polarity change.</li> </ul> <p>The valid range is 100 to 2000. The default is 1000.</p> <p><b>Note:</b> See the EnableDIDWink parameter for configuring the wink signaling type.</p>
Web/EMS: Delay Before DID Wink CLI: delay-b4-did-wink <b>[DelayBeforeDIDWink]</b>	<p>Defines the time interval (in msec) between the detection of the off-hook and the generation of the DID Wink.</p> <p>The valid range is 0 to 1,000. The default is 0.</p> <p><b>Note:</b> This parameter is applicable only to FXS interfaces.</p>
EMS: NTT DID Signalling Form CLI: NTT-DID-signaling-form <b>[NTTDIDSignallingForm]</b>	<p>Determines the type of DID signaling support for NTT (Japan) modem: DTMF- or Frequency Shift Keying (FSK)-based signaling. The devices can be connected to Japan's NTT PBX using 'Modem' DID lines. These DID lines are used to deliver a called number to the PBX.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) FSK-based signaling</li> <li><b>[1]</b> = DTMF-based signaling</li> </ul> <p><b>Note:</b> This parameter is applicable only to FXS interfaces.</p>
EMS: Enable DID <b>[EnableDID]</b>	<p>This table parameter enables support for Japan NTT 'Modem' DID. FXS interfaces can be connected to Japan's NTT PBX using 'Modem' DID lines. These DID lines are used to deliver a called number to the PBX. The DID signal can be sent alone or combined with an NTT Caller ID signal.</p> <p>The format of this parameter is as follows: <b>[EnableDID]</b></p>



Parameter	Description
	<p>FORMAT EnableDID_<b>Index</b> = EnableDID_<b>IsEnable</b>, EnableDID_Port, EnableDID_Module;  <b>[EnableDID]</b></p> <p>Where,</p> <ul style="list-style-type: none"> <li>IsEnable = Enables <b>[1]</b> or disables <b>[0]</b> (default) Japan NTT Modem DID support.</li> <li>Port = Port number.</li> <li>Module = Module number.</li> </ul> <p>For example:  EnableDID 0 = 1,1,2; (DID is enabled on Port 1 of Module 2)</p> <p><b>Note:</b> This parameter is applicable only to FXS interfaces.</p>
CLI: wink-time <b>[WinkTime]</b>	<p>Defines the time (in msec) elapsed between two consecutive polarity reversals. This parameter can be used for DID signaling, for example, E911 lines to the Public Safety Answering Point (PSAP), according to the Bellcore GR-350-CORE standard (refer to the ini file parameter Enable911PSAP).</p> <p>The valid range is 0 to 4,294,967,295. The default is 200.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable to FXS and FXO interfaces.</li> <li>For this parameter to take effect, a device reset is required.</li> </ul>

### 59.11.5.12 ISDN BRI Parameters

The automatic dialing upon off-hook parameters are described in the table below.

#### Automatic Dialing Parameters

Parameter	Description
<b>ISDN Supplementary Services Table</b>	
<p>Web: ISDN Supp Services Table</p> <p>EMS: Digital Gateway Provisioning &gt; ISDN Supplementary Services</p> <p>CLI: configure voip/gw digitalgw isdn-supp-serv  <b>[ISDNSuppServ]</b></p>	<p>This table parameter defines BRI phone extension numbers per BRI port and configures various ISDN supplementary services per BRI endpoint. The format of this parameter is as follows:</p> <p><b>[ ISDNSuppServ ]</b></p> <p>FORMAT ISDNSuppServ_Index = ISDNSuppServ_PhoneNumber, ISDNSuppServ_Module, ISDNSuppServ_Port, ISDNSuppServ_UserId, ISDNSuppServ_UserPassword, ISDNSuppServ_CallerID, ISDNSuppServ_IsPresentationRestricted, ISDNSuppServ_IsCallerIDEnabled;</p> <p><b>[ \ISDNSuppServ ]</b></p> <p>For example:</p> <p>ISDNSuppServ 0 = 400, 1, 1, user, pass, callerid, 0, 1;  ISDNSuppServ 1 = 401, 1, 1, user, pass, callerid, 0, 1;</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring ISDN BRI Supplementary Services' on page <a href="#">386</a>.</p>
<b>BRI-to-SIP Supplementary Services Codes for Call Forward</b>	
<p><b>Note:</b> Upon receipt of an ISDN Facility message for call forward from the BRI phone, the device sends a SIP INVITE to the softswitch with a user-defined code in the SIP To header, representing the reason for the call forward. For more information on BRI call forwarding, see 'BRI Call</p>	

Parameter	Description
Forwarding' on page <a href="#">357</a> .	
Web/EMS: Call Forward Unconditional <b>[SuppServCodeCFU]</b>	<p>Defines the prefix code for activating Call Forward Unconditional sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p><b>Note:</b> The string must be enclosed in single apostrophe (e.g., '*72').</p>
Web/EMS: Call Forward Unconditional Deactivation <b>[SuppServCodeCFUD eact]</b>	<p>Defines the prefix code for deactivating Call Forward Unconditional Deactivation sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p><b>Note:</b> The string must be enclosed in single apostrophe (e.g., '*72').</p>
Web: Call Forward on Busy EMS: Code Call Forward on Busy <b>[SuppServCodeCFB]</b>	<p>Defines the prefix code for activating Call Forward on Busy sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p><b>Note:</b> The string must be enclosed in single apostrophe (e.g., '*72').</p>
Web: Call Forward on Busy Deactivation EMS: Code Call Forward on Busy Deactivation <b>[SuppServCodeCFBD eact]</b>	<p>Defines the prefix code for deactivating Call Forward on Busy Deactivation sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p><b>Note:</b> The string must be enclosed in single apostrophe (e.g., '*72').</p>
Web: Call Forward on No Reply EMS: Code Call Forward on No Reply <b>[SuppServCodeCFNR]</b>	<p>Defines the prefix code for activating Call Forward on No Reply sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p><b>Note:</b> The string must be enclosed in single apostrophe (e.g., '*72').</p>
Call Forward on No Reply Deactivation EMS: Code Call Forward on No Reply Deactivation <b>[SuppServCodeCFNR Deact]</b>	<p>Defines the prefix code for deactivating Call Forward on No Reply Deactivation sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p><b>Note:</b> The string must be enclosed in single apostrophe (e.g., '*72').</p>

## 59.11.6 PSTN Parameters

This subsection describes the device's PSTN parameters.

### 59.11.6.1 General Parameters

The general PSTN parameters are described in the table below.

**General PSTN Parameters**

Parameter	Description
Web/EMS: Protocol Type CLI: protocol <b>[ProtocolType]</b>	<p>Defines the PSTN protocol for all the Trunks. To configure the protocol type for a specific Trunk, use the <i>ini</i> file parameter ProtocolType_x:</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> NONE</li> <li>▪ <b>[1]</b> E1 EURO ISDN = ISDN PRI Pan-European (CTR4) protocol</li> <li>▪ <b>[2]</b> T1 CAS = Common T1 robbed bits protocols including E&amp;M wink start, E&amp;M immediate start, E&amp;M delay dial/start and loop-start and ground start.</li> <li>▪ <b>[3]</b> T1 RAW CAS</li> <li>▪ <b>[4]</b> T1 TRANSPARENT = Transparent protocol, where no signaling is provided by the device. Timeslots 1 to 24 of all trunks are mapped to DSP channels.</li> <li>▪ <b>[5]</b> E1 TRANSPARENT 31 = Transparent protocol, where no signaling is provided by the device. Timeslots 1 to 31 of each trunk are mapped to DSP channels.</li> <li>▪ <b>[6]</b> E1 TRANSPARENT 30 = Transparent protocol, where no signaling is provided by the device. Timeslots 1 to 31, excluding time slot 16 of all trunks are mapped to DSP channels.</li> <li>▪ <b>[7]</b> E1 MFCR2 = Common E1 MFC/R2 CAS protocols (including line signaling and compelled register signaling).</li> <li>▪ <b>[8]</b> E1 CAS = Common E1 CAS protocols (including line signaling and MF/DTMF address transfer).</li> <li>▪ <b>[9]</b> E1 RAW CAS</li> <li>▪ <b>[10]</b> T1 NI2 ISDN = National ISDN 2 PRI protocol</li> <li>▪ <b>[11]</b> T1 4ESS ISDN = ISDN PRI protocol for the Lucent™/AT&amp;T™ 4ESS switch.</li> <li>▪ <b>[12]</b> T1 5ESS 9 ISDN = ISDN PRI protocol for the Lucent™/AT&amp;T™ 5ESS-9 switch.</li> <li>▪ <b>[13]</b> T1 5ESS 10 ISDN = ISDN PRI protocol for the Lucent™/AT&amp;T™ 5ESS-10 switch.</li> <li>▪ <b>[14]</b> T1 DMS100 ISDN = ISDN PRI protocol for the Nortel™ DMS switch.</li> <li>▪ <b>[15]</b> J1 TRANSPARENT</li> <li>▪ <b>[16]</b> T1 NTT ISDN = ISDN PRI protocol for the Japan - Nippon Telegraph Telephone (known also as INS 1500).</li> <li>▪ <b>[17]</b> E1 AUSTEL ISDN = ISDN PRI protocol for the Australian Telecom.</li> <li>▪ <b>[18]</b> E1 HKT ISDN = ISDN PRI (E1) protocol for the Hong Kong - HKT.</li> <li>▪ <b>[19]</b> E1 KOR ISDN = ISDN PRI protocol for Korean Operator</li> </ul>

Parameter	Description
	<p>(similar to ETSI).</p> <ul style="list-style-type: none"> <li>▪ <b>[20]</b> T1 HKT ISDN = ISDN PRI (T1) protocol for the Hong Kong - HKT.</li> <li>▪ <b>[21]</b> E1 QSIG = ECMA 143 QSIG over E1</li> <li>▪ <b>[22]</b> E1 TNZ = ISDN PRI protocol for Telecom New Zealand (similar to ETSI)</li> <li>▪ <b>[23]</b> T1 QSIG = ECMA 143 QSIG over T1</li> <li>▪ <b>[30]</b> E1 FRENCH VN6 ISDN = France Telecom VN6</li> <li>▪ <b>[31]</b> E1 FRENCH VN3 ISDN = France Telecom VN3</li> <li>▪ <b>[34]</b> T1 EURO ISDN = ISDN PRI protocol for Euro over T1</li> <li>▪ <b>[35]</b> T1 DMS100 Meridian ISDN = ISDN PRI protocol for the Nortel™ DMS Meridian switch</li> <li>▪ <b>[36]</b> T1 NI1 ISDN = National ISDN 1 PRI protocol</li> <li>▪ <b>[40]</b> E1 NI2 ISDN = National ISDN 2 PRI protocol over E1</li> <li>▪ <b>[50]</b> BRI EURO ISDN = Euro ISDN over BRI</li> <li>▪ <b>[51]</b> BRI N12 ISDN</li> <li>▪ <b>[52]</b> BRI DMS 100 ISDN</li> <li>▪ <b>[53]</b> BRI 5ESS 10 ISDN</li> <li>▪ <b>[54]</b> BRI QSIG = QSIG over BRI</li> <li>▪ <b>[55]</b> BRI VN6 = VN6 over BRI</li> <li>▪ <b>[56]</b> BRI NTT = BRI ISDN Japan (Nippon Telegraph)</li> <li>▪ <b>[57]</b> BRI IUA</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ All PRI trunks must be configured as the same line type (either E1 or T1). The device can support different variants of CAS and PRI protocols on different E1/T1 spans (no more than four simultaneous PRI variants).</li> <li>▪ BRI trunks can operate together with E1 or T1 trunks.</li> </ul>
<b>[ProtocolType_x]</b>	<p>Defines the protocol type per trunk ID (where x denotes the Trunk ID and 0 is the first trunk). For more information, see the ProtocolType parameter.</p>
<b>[ISDNTimerT310]</b>	<p>Defines the T310 override timer for DMS, Euro ISDN, and ISDN NI2 variants. An ISDN timer is started when a Q.931 Call Proceeding message is received. The timer is stopped when a Q.931 Alerting, Connect, or Disconnect message is received from the other end. If no ISDN Alerting, Progress, or Connect message is received within the duration of T310 timer, the call clears.</p> <p>The valid value range is 0 to 600 seconds. The default is 0 (i.e., use the default timer value according to the protocol's specifications).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ When both the parameters ISDNDmsTimerT310 and ISDNTimerT310 are configured, the value of the parameter ISDNTimerT310 prevails.</li> </ul>
<b>[ISDNDMSTimerT310]</b>	<p>Defines the override T310 timer for the DMS-100 ISDN variant. T310 defines the timeout between the receipt of a Proceeding message and the receipt of an Alerting/Connect message.</p> <p>The valid range is 10 to 30. The default is 10 (seconds).</p> <p><b>Notes:</b></p>

Parameter	Description
	<ul style="list-style-type: none"> <li>Instead of configuring this parameter, it is recommended to use the parameter ISDNTimerT310.</li> <li>This parameter is applicable only to Nortel DMS and Nortel MERIDIAN PRI variants (ProtocolType = 14 and 35).</li> </ul>
<b>[ISDNTimerT301]</b>	<p>Defines the override T301 timer (in seconds). The T301 timer is started when a Q.931 Alert message is received. The timer is stopped when a Q.931 Connect/Disconnect message is received from the other side. If no Connect or Disconnect message is received within the duration of T301, the call is cleared.</p> <p>The valid range is 0 to 2400. The default is 0 (i.e., the default T301 timer value - 180 seconds - is used). If set to any other value than 0, it overrides the timer with this value.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>This parameter is applicable only to the QSIG variant.</li> </ul>
<b>[ISDNJapanNTTTimerT3JA]</b>	<p>Defines the T3_JA timer (in seconds). This parameter overrides the internal PSTN T301 timeout on the Users Side (TE side). If an outgoing call from the device to ISDN is not answered during this timeout, the call is released.</p> <p>The valid range is 10 to 240. The default is 50.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This timer is also affected by the parameter PSTNAlertTimeout.</li> <li>This parameter is applicable only to the Japan NTT PRI variant (ProtocolType = 16).</li> </ul>
Web/EMS: Trace Level <b>[TraceLevel]</b>	<p>Defines the trace level:</p> <ul style="list-style-type: none"> <li><b>[0]</b> No Trace (default)</li> <li><b>[1]</b> Full ISDN Trace</li> <li><b>[2]</b> Layer 3 ISDN Trace</li> <li><b>[3]</b> Only ISDN Q.931 Messages Trace</li> <li><b>[4]</b> Layer 3 ISDN No Duplication Trace</li> </ul>
Web/EMS: Framing Method CLI: framing <b>[FramingMethod]</b>	<p>Determines the physical framing method for the trunk.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Extended Super Frame = (Default) Depends on protocol type: <ul style="list-style-type: none"> <li>✓ E1: E1 CRC4 MultiFrame Format extended G.706B (same as c)</li> <li>✓ T1: T1 Extended Super Frame with CRC6 (same as D)</li> </ul> </li> <li><b>[1]</b> Super Frame = T1 SuperFrame Format (as B).</li> <li><b>[a]</b> E1 FRAMING DDF = E1 DoubleFrame Format - CRC4 is forced to off</li> <li><b>[b]</b> E1 FRAMING MFF CRC4 = E1 CRC4 MultiFrame Format - CRC4 is always on</li> <li><b>[c]</b> E1 FRAMING MFF CRC4 EXT = E1 CRC4 MultiFrame Format extended G.706B - auto negotiation is on. If the negotiation fails, it changes automatically to CRC4 off (ddf)</li> <li><b>[A]</b> T1 FRAMING F4 = T1 4-Frame multiframe.</li> <li><b>[B]</b> T1 FRAMING F12 = T1 12-Frame multiframe (D4).</li> <li><b>[C]</b> T1 FRAMING ESF = T1 Extended SuperFrame without CRC6</li> <li><b>[D]</b> T1 FRAMING ESF CRC6 = T1 Extended SuperFrame with</li> </ul>

Parameter	Description
	<p>CRC6</p> <ul style="list-style-type: none"> <li>▪ <b>[E]</b> T1 FRAMING F72 = T1 72-Frame multiframe (SLC96)</li> <li>▪ <b>[F]</b> T1 FRAMING ESF CRC6 J2 = J1 Extended SuperFrame with CRC6 (Japan)</li> </ul> <p><b>Note:</b> This parameter is not configurable for BRI interfaces; the device automatically uses the BRI framing method.</p>
<b>[FramingMethod_x]</b>	<p>Same as the description for parameter FramingMethod, but for a specific trunk ID (where x denotes the Trunk ID and 0 is the first Trunk).</p>
<p>Web/EMS: Clock Master CLI: clock-master <b>[ClockMaster]</b></p>	<p>Determines the Tx clock source of the E1/T1 line.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Recovered = (Default) Generate the clock according to the Rx of the E1/T1 line.</li> <li>▪ <b>[1]</b> Generated = Generate the clock according to the internal TDM bus.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The source of the internal TDM bus clock is determined by the parameter TDMBusClockSource.</li> <li>▪ This parameter is not applicable to BRI interfaces.</li> </ul>
<b>[ClockMaster_x]</b>	<p>Same as the description for parameter ClockMaster, but for a specific Trunk ID (where x denotes the Trunk ID and 0 is the first Trunk).</p> <p><b>Note:</b> This parameter is not applicable to BRI interfaces.</p>
<p>Web/EMS: Line Code CLI: line-code <b>[LineCode]</b></p>	<p>Selects B8ZS or AMI for T1 spans, and HDB3 or AMI for E1 spans.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> B8ZS = (Default) B8ZS line code (for T1 trunks only).</li> <li>▪ <b>[1]</b> AMI = AMI line code.</li> <li>▪ <b>[2]</b> HDB3 = HDB3 line code (for E1 trunks only).</li> </ul> <p><b>Note:</b> This parameter is not configurable for BRI interfaces; the device automatically uses the Modified Alternate Mark Invert (MAMI) line code.</p>
<b>[LineCode_x]</b>	<p>Same as the description for parameter LineCode, but for a specific trunk ID (where 0 denotes the first trunk).</p>
<b>[AdminState]</b>	<p>Defines the administrative state for all trunks.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Lock the trunk; stops trunk traffic to configure the trunk protocol type.</li> <li>▪ <b>[1]</b> = Shutting down (read only).</li> <li>▪ <b>[2]</b> = (Default) Unlock the trunk; enables trunk traffic.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ When the device is locked from the Web interface, this parameter changes to 0.</li> <li>▪ To define the administrative state per trunk, use the TrunkAdministrativeState parameter.</li> </ul>
<b>[TrunkAdministrativeState_x]</b>	<p>Defines the administrative state per trunk, where x denotes the trunk number.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Lock the trunk; stops trunk traffic to configure the trunk protocol type.</li> <li>▪ <b>[1]</b> = shutting down (read only).</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li><b>[2]</b> = (Default) Unlock the trunk; enables trunk traffic.</li> </ul>
Web/EMS: Line Build Out Loss CLI: line-build-out-loss <b>[LineBuildOut.Loss]</b>	<p>Defines the line build out loss for the selected T1 trunk.</p> <ul style="list-style-type: none"> <li><b>[0]</b> 0 dB (default)</li> <li><b>[1]</b> -7.5 dB</li> <li><b>[2]</b> -15 dB</li> <li><b>[3]</b> -22.5 dB</li> </ul> <p><b>Note:</b> This parameter is applicable only to T1 trunks.</p>
<b>[TDMHairPinning]</b>	<p>Defines static TDM hair-pinning (cross-connection) performed at initialization. The connection is between trunks with an option to exclude a single B-channel in each trunk. Format example: T0-T1/B3,T2-T3,T4-T5/B2.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Enable TDM Tunneling EMS: TDM Over IP CLI: tdm-tunneling <b>[EnableTDMoverIP]</b>	<p>Enables TDM tunneling.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>When TDM Tunneling is enabled, the originating device automatically initiates SIP calls from all enabled B-channels pertaining to E1/T1/J1 spans that are configured with the 'Transparent' protocol. The called number of each call is the internal phone number of the B-channel from where the call originates. The 'The Inbound IP Routing Table is used to define the destination IP address of the terminating device. The terminating device automatically answers these calls if its E1/T1 protocol is set to 'Transparent' (ProtocolType = 5).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For an overview on TDM tunneling, see 'TDM Tunneling' on page 279.</li> </ul>

### 59.11.6.2 TDM Bus and Clock Timing Parameters

The TDM Bus parameters are described in the table below.

**TDM Bus and Clock Timing Parameters**

Parameter	Description
<b>TDM Bus Parameters</b>	
Web/EMS: PCM Law Select <b>[PCMLawSelect]</b>	<p>Determines the type of pulse-code modulation (PCM) companding algorithm law in input and output TDM bus.</p> <ul style="list-style-type: none"> <li><b>[1]</b> Alaw</li> <li><b>[3]</b> MuLaw</li> </ul> <p>The default is automatically selected according to the Protocol Type of the selected trunk: E1 defaults to ALaw, T1 defaults to MuLaw. If the Protocol Type is set to NONE, the default is MuLaw.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>Typically, A-Law is used for E1 spans and Mu-Law for T1/J1</li> </ul>



Parameter	Description
	spans.
Web/EMS: Idle PCM Pattern CLI: idle-pcm-pattern <b>[IdlePCMPattern]</b>	<p>Defines the PCM Pattern that is applied to the E1/T1 timeslot (B-channel) when the channel is idle.</p> <p>The range is 0 to 255. The default is set internally according to the Law select 1 (0xFF for Mu-Law; 0x55 for A-law).</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web/EMS: Idle ABCD Pattern <b>[IdleABCDPattern]</b>	<p>Defines the ABCD (CAS) Pattern that is applied to the CAS signaling bus when the channel is idle.</p> <p>The valid range is 0x0 to 0xF. The default is -1 (i.e., default pattern is 0000).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>This parameter is applicable only when using PSTN interface with CAS protocols.</li> </ul>
Web/EMS: TDM Bus Clock Source <b>[TDMBusClockSource]</b>	<p>Determines the clock source to which the device synchronizes.</p> <ul style="list-style-type: none"> <li><b>[1]</b> Internal = (Default) Generate clock from local source.</li> <li><b>[4]</b> Network = Recover clock from PSTN line.</li> </ul>
Web/EMS: TDM Bus Local Reference <b>[TDMBusLocalReference]</b>	<p>Defines the physical Trunk ID from which the device recovers (receives) its clock synchronization.</p> <p>The range is 0 to the maximum number of Trunks. The default is 0.</p> <p><b>Note:</b> This parameter is applicable only if the parameter TDMBusClockSource is set to 4 and the parameter TDMBusPSTNAutoClockEnable is set to 0.</p>
Web/EMS: TDM Bus Enable Fallback <b>[TDMBusEnableFallback]</b>	<p>Defines the automatic fallback of the clock.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Manual (default)</li> <li><b>[1]</b> Auto Non-Revertive</li> <li><b>[2]</b> Auto Revertive</li> </ul>
Web: TDM Bus Fallback Clock Source EMS: TDM Bus Fallback Clock <b>[TDMBusFallbackClock]</b>	<p>Determines the fallback clock source on which the device synchronizes in the event of a clock failure.</p> <ul style="list-style-type: none"> <li><b>[4]</b> Network (default)</li> <li><b>[8]</b> H.110_A</li> <li><b>[9]</b> H.110_B</li> <li><b>[10]</b> NetReference1</li> <li><b>[11]</b> NetReference2</li> </ul>
Web/EMS: TDM Bus Net Reference Speed <b>[TDMBusNetrefSpeed]</b>	<p>Defines the NetRef frequency (for both generation and synchronization).</p> <ul style="list-style-type: none"> <li><b>[0]</b> 8 kHz (default)</li> <li><b>[1]</b> 1.544 MHz</li> <li><b>[2]</b> 2.048 MHz</li> </ul>
Web: TDM Bus PSTN Auto FallBack Clock EMS: TDM Bus Auto Fall Back Enable <b>[TDMBusPSTNAutoClockEnable]</b>	<p>Enables the PSTN trunk Auto-Fallback Clock feature.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Recovers the clock from the E1/T1 line defined by the parameter TDMBusLocalReference.</li> <li><b>[1]</b> Enable = Recovers the clock from any connected synchronized slave E1/T1 line. If this trunk loses its synchronization, the device attempts to recover the clock from the next trunk. Note that initially, the device attempts to</li> </ul>



Parameter	Description
	<p>recover the clock from the trunk defined by the parameter TDMBusLocalReference.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>This parameter is relevant only if the parameter TDMBusClockSource is set to 4.</li> </ul>
Web: TDM Bus PSTN Auto Clock Reverting EMS: TDM Bus Auto Fall Back Reverting Enable <b>[TDMBusPSTNAutoClockRevertingEnable]</b>	<p>Enables the PSTN trunk Auto-Fallback Reverting feature. If enabled and a trunk returning to service has an AutoClockTrunkPriority parameter value that is higher than the priority of the local reference trunk (set in the TDMBusLocalReference parameter), the local reference reverts to the trunk with the higher priority that has returned to service for the device's clock source.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>This parameter is applicable only when the TDMBusPSTNAutoClockEnable parameter is set to 1.</li> </ul>
Web: Auto Clock Trunk Priority EMS: Auto Trunk Priority CLI: clock-priority <b>[AutoClockTrunkPriority]</b>	<p>Defines the trunk priority for auto-clock fallback (per trunk parameter).</p> <ul style="list-style-type: none"> <li>0 to 99 = priority, where 0 (default) is the highest.</li> <li>100 = the SW never performs a fallback to that trunk (usually used to mark untrusted source of clock).</li> </ul> <p><b>Note:</b> Fallback is enabled when the TDMBusPSTNAutoClockEnable parameter is set to 1.</p>

### 59.11.6.3 CAS Parameters

The Common Channel Associated (CAS) parameters are described in the table below. Note that CAS is not applicable to BRI interfaces.

#### CAS Parameters

Parameter	Description
Web: CAS Transport Type EMS: CAS Relay Transport Mode CLI: CAS-transport-type <b>[CASTransportType]</b>	<p>Determines the ABCD signaling transport type over IP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> CAS Events Only = (Default) Disable CAS relay.</li> <li><b>[1]</b> CAS RFC2833 Relay = Enable CAS relay mode using RFC 2833.</li> </ul> <p>The CAS relay mode can be used with the TDM tunneling feature to enable tunneling over IP for both voice and CAS signaling bearers.</p>
<b>[CASAddressingDelimiters]</b>	<p>Enables the addition of delimiters to the received address or received ANI digits string.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (default) Disable. The address and ANI strings remain without delimiters.</li> <li><b>[1]</b> = Enable. Delimiters such as '*', '#', and 'ST' are added to the received address or received ANI digits string.</li> </ul>

Parameter	Description
CLI: cas-delimiters-types <b>[CASDelimitersPaddingUsage]</b>	<p>Defines the digits string delimiter padding usage per trunk.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Default address string padding: '*XXX#' (where XXX is the digit string that begins with '*' and ends with '#', when using padding).</li> <li><b>[1]</b> = Special use of asterisks delimiters: '*XXX*YYY*' (where XXX is the address, YYY is the source phone number, and '*' is the only delimiter padding).</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: CAS Table per Trunk EMS: Trunk CAS Table Index CLI: cas-table-index <b>[CASTableIndex_x]</b>	<p>Defines the CAS protocol per trunk from a list of CAS protocols defined by the parameter CASFileName_x.</p> <p>For example, the below configuration specifies Trunks 0 and 1 to use the E&amp;M Winkstart CAS (E_M_WinkTable.dat) protocol, and Trunks 2 and 3 to use the E&amp;M Immediate Start CAS (E_M_ImmediateTable.dat) protocol:</p> <pre> CASFileName_0 = 'E_M_WinkTable.dat' CASFileName_1 = 'E_M_ImmediateTable.dat' CASTableIndex_0 = 0 CASTableIndex_1 = 0 CASTableIndex_2 = 1 CASTableIndex_3 = 1           </pre> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>You can define CAS tables per B-channel using the parameter CASChannelIndex.</li> <li>The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.</li> </ul>
Web: Dial Plan EMS: Dial Plan Name CLI: cas-dial-plan-name <b>[CASTrunkDialPlanName_x]</b>	<p>Defines the CAS Dial Plan name per trunk.</p> <p>The range is up to 11 characters.</p> <p>For example, the below configures E1_MFCR2 trunk with a single protocol (Trunk 5):</p> <pre> ProtocolType_5 = 7 CASFileName_0='R2_Korea_CP_ANI.dat' CASTableIndex_5 = 0 DialPlanFileName = 'DialPlan_USA.dat' CASTrunkDialPlanName_5 = 'AT_T'           </pre> <p><b>Note:</b> The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.</p>
<b>[CASFileName_x]</b>	<p>Defines the CAS file name (e.g., 'E_M_WinkTable.dat') that defines the CAS protocol, where x denotes the CAS file ID (0-7). It is possible to define up to eight different CAS files by repeating this parameter. Each CAS file can be associated with one or more of the device's trunks, using the parameter CASTableIndex_x.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web/EMS: CAS Table per Channel CLI: cas-channel-index <b>[CASChannelIndex]</b>	<p>Defines the loaded CAS protocol table index per B-channel pertaining to a CAS trunk. This parameter is assigned a string value and can be set in one of the following two formats:</p> <ul style="list-style-type: none"> <li><b>CAS table per channel:</b> Each channel is separated by a comma and the value entered denotes the CAS table index used for that channel. The syntax is &lt;CAS index&gt;,&lt;CAS index&gt; (e.g., "1,2,1,2..."). For this format, 31 indices must be defined for E1 trunks (including dummy for B-channel 16), or 24 indices for T1 trunks. Below is an example for configuring a</li> </ul>

Parameter	Description
	<p>T1 CAS trunk (Trunk 5) with several CAS variants:</p> <pre> ProtocolType_5 = 7 CASFILENAME_0='E_M_FGBWinkTable.dat' CASFILENAME_1='E_M_FGDWinkTable.dat' CASFILENAME_2='E_M_WinkTable.txt' CasChannelIndex_5 = '0,0,0,1,1,1,2,2,2,0,0,0,1,1,1,0,1,2,0,2,1,2,2,2' CASDelimitersPaddingUsage_5 = 1 </pre> <ul style="list-style-type: none"> <li> <b>CAS table per channel group:</b> Each channel group is separated by a colon and each channel is separated by a comma. The syntax is &lt;x-y channel range&gt;:&lt;CAS table index&gt;, (e.g., "1-10:1,11-31:3"). Every B-channel (including 16 for E1) must belong to a channel group. Below is an example for configuring an E1 CAS trunk (Trunk 5) with several CAS variants: <pre> ProtocolType_5 = 8 CASFILENAME_2='E1_R2D' CASFILENAME_7='E_M_ImmediateTable_A-Bit.txt' CasChannelIndex_5 = '1-10:2,11-20:7,21-31:2' </pre> </li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To configure this parameter, the trunk must first be stopped.</li> <li>Only one of these formats can be implemented; not both.</li> <li>When this parameter is not configured, a single CAS table for the entire trunk is used, configured by the parameter CASTableIndex.</li> </ul>
[CASTablesNum]	<p>Defines how many CAS protocol configurations files are loaded. The valid range is 1 to 8.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>CAS State Machines Parameters</b> <p><b>Note:</b> For configuring the CAS State Machine table using the Web interface, see 'Configuring CAS State Machines' on page 276. The CAS state machine can be configured only through the Web-based management tool.</p>	
Web: Generate Digit On Time [CASStateMachineGenerateDigitOnTime]	<p>Generates digit on-time (in msec). The value must be a positive value. The default is -1.</p>
Web: Generate Inter Digit Time [CASStateMachineGenerateInterDigitTime]	<p>Generates digit off-time (in msec). The value must be a positive value. The default is -1.</p>
Web: DTMF Max Detection Time [CASStateMachineDTMFMaxOnDetectionTime]	<p>Detects digit maximum on time (according to DSP detection information event) in msec units. The value must be a positive value. The default is -1.</p>
Web: DTMF Min Detection Time [CASStateMachineDTMFMinOnDetectionTime]	<p>Detects digit minimum on time (according to DSP detection information event) in msec units. The digit time length must be longer than this value to receive a detection. Any number may be used, but the value must be less than CasStateMachineDTMFMaxOnDetectionTime. The value must be a positive value. The default is -1.</p>
Web: MAX Incoming Address	<p>Defines the limitation for the maximum address digits that need to</p>

Parameter	Description
Digits [CASStateMachineMaxNumOfIncomingAddressDigits]	be collected. After reaching this number of digits, the collection of address digits is stopped. The value must be an integer. The default is -1.
Web: MAX Incoming ANI Digits [CASStateMachineMaxNumOfIncomingANIDigits]	Defines the limitation for the maximum ANI digits that need to be collected. After reaching this number of digits, the collection of ANI digits is stopped. The value must be an integer. The default is -1.
Web: Collect ANI [CASStateMachineCollectANI]	In some cases, when the state machine handles the ANI collection (not related to MFCR2), you can enable the state machine to collect ANI or discard ANI. <ul style="list-style-type: none"> <li>▪ [0] No = Don't collect ANI.</li> <li>▪ [1] Yes = Collect ANI.</li> <li>▪ [-1] Default = Default value.</li> </ul>
Web: Digit Signaling System [CASStateMachineDigitSignalingSystem]	Defines which Signaling System to use in both directions (detection\generation). <ul style="list-style-type: none"> <li>▪ [0] DTMF = DTMF signaling.</li> <li>▪ [1] MF = (Default) MF signaling.</li> <li>▪ [-1] Default = Default value.</li> </ul>

#### 59.11.6.4 ISDN Parameters

The ISDN parameters are described in the table below.

**ISDN Parameters**

Parameter	Description
Web: ISDN Termination Side EMS: Termination Side CLI: isdn-termination-side [TerminationSide]	Determines the ISDN termination side. <ul style="list-style-type: none"> <li>▪ [0] User side = (Default) ISDN User Termination Equipment (TE) side.</li> <li>▪ [1] Network side = ISDN Network Termination (NT) side.</li> </ul> <p><b>Note:</b> Select 'User side' when the PSTN or PBX side is configured as 'Network side' and vice versa. If you don't know the device's ISDN termination side, choose 'User side'. If the D-channel alarm is indicated, choose 'Network Side'.</p> <p>The BRI module supports the ITU-T I.430 standard, which defines the ISDN-BRI layer 1 specification. The BRI and PRI ports are configured similarly, using this parameter. When an NT port is active, it drives a 38-V line and sends an INFO1 signal (as defined in ITU-T I.430 Table 4) on the data line to synchronize to a TE port that might be connected to it. To stop the voltage and the INFO1 signal on the line, stop the trunk using the Stop Trunk button.</p>
[TerminationSide_x]	Same as the description for parameter TerminationSide, but for a specific trunk ID (where x denotes the Trunk ID and 0 is the first Trunk).
BRI Layer 2 Mode CLI: isdn-layer2-mode [BriLayer2Mode]	Determines whether Point-to-Point or Point-to-Multipoint mode for BRI ports. <ul style="list-style-type: none"> <li>▪ [0] Point to Point (default)</li> <li>▪ [1] Point to Multipoint = Must be configured for Network side.</li> </ul>

Parameter	Description
Web/EMS: B-channel Negotiation CLI: b-ch-negotiation <b>[BchannelNegotiation]</b>	<p>Determines the ISDN B-Channel negotiation mode.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Preferred</li> <li>▪ <b>[1]</b> Exclusive (default)</li> <li>▪ <b>[2]</b> Any</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to ISDN protocols.</li> <li>▪ For some ISDN variants, when 'Any' (2) is selected, the Setup message excludes the Channel Identification IE.</li> <li>▪ The 'Any' (2) option is applicable only if the following conditions are met: <ul style="list-style-type: none"> <li>✓ The parameter TerminationSide is set to 0 ('User side').</li> <li>✓ The PSTN protocol type (ProtocolType) is configured as Euro ISDN.</li> </ul> </li> </ul>
<b>NFAS Parameters</b> <b>Note:</b> These parameters are applicable to PRI interfaces.	
Web: NFAS Group Number EMS: Group Number CLI: isdn-nfas-group-number <b>[NFASGroupNumber_x]</b>	<p>Defines the ISDN Non-Facility Associated Signaling (NFAS) group number (NFAS member) per trunk.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Non-NFAS trunk.</li> <li>▪ <b>[1] to [12]</b> = NFAS group number.</li> </ul> <p>Trunks that belong to the same NFAS group have the same number. With NFAS, you can use a single D-channel to control multiple PRI interfaces.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ This parameter is applicable only to T1 ISDN protocols.</li> <li>▪ The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.</li> <li>▪ For more information on NFAS, see 'ISDN Non-Facility Associated Signaling (NFAS)' on page <a href="#">283</a>.</li> </ul>
Web/EMS: D-channel Configuration CLI: isdn-nfas-dchannel-type <b>[DChConfig_x]</b>	<p>Defines primary, backup (optional), and B-channels only, per trunk.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] PRIMARY</b> = (Default) Primary Trunk - contains a D-channel that is used for signaling.</li> <li>▪ <b>[1] BACKUP</b> = Backup Trunk - contains a backup D-channel that is used if the primary D-channel fails.</li> <li>▪ <b>[2] NFAS</b> = NFAS Trunk - contains only 24 B-channels, without a signaling D-channel.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to T1 ISDN protocols.</li> <li>▪ The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.</li> </ul>
Web: NFAS Interface ID EMS: ISDN NFAS Interface ID CLI: isdn-nfas-interface-id <b>[ISDNNFASInterfaceID_x]</b>	<p>Defines a different Interface ID per T1 trunk.</p> <p>The valid range is 0 to 100. The default interface ID equals the trunk's ID.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To set the NFAS interface ID, configure ISDNIBehavior_x to include '512' feature per T1 trunk.</li> <li>▪ The x in the ini file parameter denotes the trunk number,</li> </ul>

Parameter	Description
	<p>where 0 is Trunk 1.</p> <ul style="list-style-type: none"> <li>For more information on NFAS, see 'ISDN Non-Facility Associated Signaling (NFAS)' on page 283.</li> </ul>
Web: Enable ignoring ISDN Disconnect with PI CLI: ign-isdn-disc-w-pi <b>[KeepISDNCallOnDisconnect WithPI]</b>	<p>Allows the device to ignore ISDN Disconnect messages with PI 1 or 8.</p> <ul style="list-style-type: none"> <li><b>[1]</b> = The call (in connected state) is not released if a Q.931 Disconnect with PI (PI = 1 or 8) message is received during the call.</li> <li><b>[0]</b> = (Default) The call is disconnected.</li> </ul>
Web: PI For Setup Message CLI: pi-4-setup-msg <b>[PIForSetupMsg]</b>	<p>Determines whether and which Progress Indicator (PI) information element (IE) is added to the sent ISDN Setup message. Some ISDN protocols such as Euro ISDN can optionally contain PI = 1 or PI = 3 in the Setup message.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = PI is not added (default).</li> <li><b>[1]</b> = PI 1 is added to a sent ISDN Setup message - call is not end-to-end ISDN.</li> <li><b>[3]</b> = PI 3 is added to a sent ISDN Setup message - calling equipment is not ISDN.</li> </ul>
<b>ISDN Flexible Behavior Parameters</b> ISDN protocol is implemented in different switches/PBXs by different vendors. Several implementations may vary slightly from the specification. Therefore, to provide a flexible interface that supports these ISDN variants, the ISDN behavior parameters can be used.	
Web/EMS: Incoming Calls Behavior CLI: isdn-bits-incoming-calls-behavior <b>[ISDNInCallsBehavior]</b>	<p>Determines the bit-field used to determine several behavior options that influence how the ISDN Stack INCOMING calls behave.</p> <ul style="list-style-type: none"> <li><b>[32]</b> DATA CONN RS = The device automatically sends a Q.931 Connect (answer) message on incoming Tel calls (Q.931 Setup).</li> <li><b>[64]</b> VOICE CONN RS = The device sends a Connect (answer) message on incoming Tel calls.</li> <li><b>[2048]</b> CHAN ID IN FIRST RS = (Default) The device sends Channel ID in the first response to an incoming Q.931 Call Setup message. Otherwise, the Channel ID is sent only if the device requires changing the proposed Channel ID.</li> <li><b>[4096]</b> USER SETUP ACK = The Setup Ack message is sent by the SIP Gateway application layer and not automatically by the PSTN stack. By default, this bit is set.</li> <li><b>[8192]</b> CHAN ID IN CALL PROC = The device sends Channel ID in a Q.931 Call Proceeding message.</li> <li><b>[65536]</b> PROGR IND IN SETUP ACK = The device includes Progress Indicator (PI=8) in Setup Ack message if an empty called number is received in an incoming Setup message. This option is applicable to the overlap dialing mode. The device also plays a dial tone (for TimeForDialTone) until the next called number digits are received. By default, this bit is set.</li> <li><b>[2147483648]</b> USER SCREEN INDICATOR = When the device receives two Calling Number IE's in the Setup message, the device, by default, uses only one of the numbers according to the following: <ul style="list-style-type: none"> <li>✓ Network provided, Network provided - the first calling number is used</li> <li>✓ Network provided, User provided: the first one is used</li> <li>✓ User provided, Network provided: the second one is used</li> </ul> </li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>✓ User provided, user provided: the first one is used</li> </ul> <p>When this bit is configured, the device behaves as follows:</p> <ul style="list-style-type: none"> <li>✓ Network provided, Network provided: the first calling number is used</li> <li>✓ Network provided, User provided: the second one is used</li> <li>✓ User provided, Network provided: the first one is used</li> <li>✓ User provided, user provided: the first one is used</li> </ul> <p><b>Note:</b> When using the <i>ini</i> file to configure the device to support several ISDNInCallsBehavior features, enter a summation of the individual feature values. For example, to support both <b>[2048]</b> and <b>[65536]</b> features, set ISDNInCallsBehavior = 67584 (i.e., 2048 + 65536).</p>
<b>[ISDNInCallsBehavior_x]</b>	Same as the description for the parameter ISDNInCallsBehavior, but per trunk (i.e., where x denotes the Trunk ID).
<p>Web/EMS: Q.931 Layer Response Behavior CLI: isdn-bits-ns-behavior <b>[ISDNIBehavior]</b></p>	<p>Bit-field used to determine several behavior options that influence the behaviour of the Q.931 protocol.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default).</li> <li>▪ <b>[1]</b> NO STATUS ON UNKNOWN IE = Q.931 Status message isn't sent if Q.931 received message contains an unknown/unrecognized IE. By default, the Status message is sent. <b>Note:</b> This value is applicable only to ISDN variants in which sending of Status message is optional.</li> <li>▪ <b>[2]</b> NO STATUS ON INV OP IE = Q.931 Status message isn't sent if an optional IE with invalid content is received. By default, the Status message is sent. <b>Note:</b> This option is applicable only to ISDN variants in which sending of Status message is optional.</li> <li>▪ <b>[4]</b> ACCEPT UNKNOWN FAC IE = Accepts unknown/unrecognized Facility IE. Otherwise, the Q.931 message that contains the unknown Facility IE is rejected (default). <b>Note:</b> This option is applicable only to ISDN variants where a complete ASN1 decoding is performed on Facility IE.</li> <li>▪ <b>[128]</b> SEND USER CONNECT ACK = The Connect ACK message is sent in response to received Q.931 Connect; otherwise, the Connect ACK is not sent. <b>Note:</b> This option is applicable only to Euro ISDN User side outgoing calls.</li> <li>▪ <b>[512]</b> EXPLICIT INTERFACE ID = Enables to configure T1 NFAS Interface ID (refer to the parameter ISDNNFASInterfaceID_x). <b>Note:</b> This value is applicable only to 4/5ESS, DMS, NI-2 and HKT variants.</li> <li>▪ <b>[2048]</b> ALWAYS EXPLICIT = Always set the Channel Identification IE to explicit Interface ID, even if the B-channel is on the same trunk as the D-channel. <b>Note:</b> This value is applicable only to 4/5ESS, DMS variants.</li> <li>▪ <b>[32768]</b> ACCEPT MU LAW =Mu-Law is also accepted in ETSI.</li> <li>▪ <b>[65536]</b> EXPLICIT PRES SCREENING = The calling party number (octet 3a) is always present even when presentation and screening are at their default. <b>Note:</b> This option is applicable only to ETSI, NI-2, and 5ESS.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[131072]</b> STATUS INCOMPATIBLE STATE = Clears the call on receipt of Q.931 Status with incompatible state. Otherwise, no action is taken (default).</li> <li>▪ <b>[262144]</b> STATUS ERROR CAUSE = Clear call on receipt of Status according to cause value.</li> <li>▪ <b>[524288]</b> ACCEPT A LAW =A-Law is also accepted in 5ESS.</li> <li>▪ <b>[2097152]</b> RESTART INDICATION = Upon receipt of a Restart message, acEV_PSTN_RESTART_CONFIRM is generated.</li> <li>▪ <b>[4194304]</b> FORCED RESTART = On data link (re)initialization, send RESTART if there is no call.</li> <li>▪ <b>[67108864]</b> NS ACCEPT ANY CAUSE = Accept any Q.850 Cause IE from ISDN. <b>Note:</b> This option is applicable only to Euro ISDN.</li> <li>▪ <b>[134217728]</b> NS_BRI_DL_ALWAYS_UP (0x08000000) = By default, the BRI D-channel goes down if there are no active calls. If this option is configured, the BRI D-channel is always up and synchronized.</li> <li>▪ <b>[536870912]</b> Alcatel coding for redirect number and display name is accepted by the device. <b>Note:</b> This option is applicable only to QSIG (and relevant for specific Alcatel PBXs such as OXE).</li> <li>▪ <b>[1073741824]</b> QSI ENCODE INTEGER = If this bit is set, INTEGER ASN.1 type is used in operator coding (compliant to new ECMA standards); otherwise, OBJECT IDENTIFIER ASN.1 type is used. <b>Note:</b> This option is applicable only to QSIG.</li> <li>▪ <b>[2147483648]</b> 5ESS National Mode For Bch Maintenance = Use the National mode of AT&amp;T 5ESS for B-channel maintenance.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To configure the device to support several ISDNBehavior features, enter a summation of the individual feature values. For example, to support both <b>[512]</b> and <b>[2048]</b> features, set the parameter ISDNBehavior is set to 2560 (i.e., 512 + 2048).</li> <li>▪ When configuring in the Web interface, to select the options click the arrow button and then for each required option select 1 to enable.</li> </ul>
<b>[ISDNBehavior_x]</b>	Same as the description for parameter ISDNBehavior, but for a specific trunk ID.
Web: General Call Control Behavior EMS: General CC Behavior CLI: isdn-bits-cc-behavior <b>[ISDNGeneralCCBehavior]</b>	Bit-field for determining several general CC behavior options. To select the options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable). <ul style="list-style-type: none"> <li>▪ <b>[2]</b> = Data calls with interworking indication use 64 kbps B-channels (physical only).</li> <li>▪ <b>[8]</b> REVERSE CHAN ALLOC ALGO = Channel ID allocation algorithm.</li> <li>▪ <b>[16]</b> = The device clears down the call if it receives a NOTIFY message specifying 'User-Suspended'. A NOTIFY (User-Suspended) message is used by some networks (e.g., in Italy or Denmark) to indicate that the remote user has cleared the call, especially in the case of a long distance voice call.</li> <li>▪ <b>[32]</b> CHAN ID 16 ALLOWED = Applies only to ETSI E1 lines (30B+D). Enables handling the differences between the newer</li> </ul>



Parameter	Description
	<p>QSIG standard (ETS 300-172) and other ETSI-based standards (ETS 300-102 and ETS 300-403) in the conversion of B-channel ID values into timeslot values:</p> <ul style="list-style-type: none"> <li>✓ In 'regular ETSI' standards, the timeslot is identical to the B-channel ID value, and the range for both is 1 to 15 and 17 to 31. The D-channel is identified as channel-id #16 and carried into the timeslot #16.</li> <li>✓ In newer QSIG standards, the channel-id range is 1 to 30, but the timeslot range is still 1 to 15 and 17 to 31. The D-channel is not identified as channel-id #16, but is still carried into the timeslot #16.</li> </ul> <p>When this bit is set, the channel ID #16 is considered as a valid B-channel ID, but timeslot values are converted to reflect the range 1 to 15 and 17 to 31. This is the new QSIG mode of operation. When this bit is not set (default), the channel_id #16 is not allowed, as for all ETSI-like standards.</p> <ul style="list-style-type: none"> <li>▪ <b>[64]</b> USE T1 PRI = PRI interface type is forced to T1.</li> <li>▪ <b>[128]</b> USE E1 PRI = PRI interface type is forced to E1.</li> <li>▪ <b>[256]</b> START WITH B CHAN OOS = B-channels start in the Out-Of-Service state (OOS).</li> <li>▪ <b>[512]</b> CHAN ALLOC LOWEST = CC allocates B-channels starting from the lowest available B-channel id.</li> <li>▪ <b>[1024]</b> CHAN ALLOC HIGHEST = CC allocates B-channels starting from the highest available B-channel id.</li> <li>▪ <b>[16384]</b> CC_TRANSPARENT_UUI bit: The UUI-protocol implementation of CC is disabled allowing the application to freely send UUI elements in any primitive, regardless of the UUI-protocol requirements (UUI Implicit Service 1). This allows more flexible application control on the UUI. When this bit is not set (default behavior), CC implements the UUI-protocol as specified in the ETS 300-403 standards for Implicit Service 1.</li> <li>▪ <b>[65536]</b> GTD5 TBCT = CC implements the VERIZON-GTD-5 Switch variant of the TBCT Supplementary Service, as specified in FSD 01-02-40AG Feature Specification Document from Verizon. Otherwise, TBCT is implemented as specified in GR-2865-CORE specification (default behavior).</li> </ul> <p><b>Note:</b> When using the <i>ini</i> file to configure the device to support several ISDNGeneralCCBehavior features, add the individual feature values. For example, to support both <b>[16]</b> and <b>[32]</b> features, set ISDNGeneralCCBehavior = 48 (i.e., 16 + 32).</p>
<p>Web/EMS: Outgoing Calls Behavior  CLI: isdn-bits-outgoing-calls-behavior  <b>[ISDNOutCallsBehavior]</b></p>	<p>Determines several behaviour options (bit fields) that influence the behaviour of the ISDN Stack outgoing calls. To select options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable).</p> <ul style="list-style-type: none"> <li>▪ <b>[2]</b> USER SENDING COMPLETE = The default behavior of the device (when this bit is not set) is to automatically generate the Sending-Complete IE in the Setup message. This behavior is used when overlap dialing is not needed. When overlap dialing is needed, set this bit and the behavior is changed to suit the scenario, i.e., Sending-Complete IE is added when required in the Setup message for Enblock mode or in the last Digit with Overlap mode.</li> <li>▪ <b>[16]</b> USE MU LAW = The device sends G.711-m-Law in</li> </ul>

Parameter	Description
	<p>outgoing voice calls. When disabled, the device sends G.711-A-Law in outgoing voice calls.</p> <p><b>Note:</b> This option is applicable only to the Korean variant.</p> <ul style="list-style-type: none"> <li>▪ <b>[128] DIAL WITH KEYPAD</b> = The device uses the Keypad IE to store the called number digits instead of the CALLED_NB IE.</li> </ul> <p><b>Note:</b> This option is applicable only to the Korean variant (Korean network). This is useful for Korean switches that don't accept the CALLED_NB IE.</p> <ul style="list-style-type: none"> <li>▪ <b>[256] STORE CHAN ID IN SETUP</b> = The device forces the sending of a Channel-Id IE in an outgoing Setup message even if it's not required by the standard (i.e., optional) and no Channel-Id has been specified in the establishment request. This is useful for improving required compatibility with switches. On BRI lines, the Channel-Id IE indicates 'any channel'. On PRI lines it indicates an unused channel ID, preferred only.</li> <li>▪ <b>[572] USE A LAW</b> = The device sends G.711 A-Law in outgoing voice calls. When disabled, the device sends the default G.711-Law in outgoing voice calls.</li> </ul> <p><b>Note:</b> This option is applicable only to the E10 variant.</p> <ul style="list-style-type: none"> <li>▪ <b>[1024]</b> = Numbering plan/type for T1 IP-to-Tel calling numbers are defined according to the manipulation tables or according to the RPID header (default). Otherwise, the plan/type for T1 calls are set according to the length of the calling number.</li> <li>▪ <b>[2048]</b> = The device accepts any IA5 character in the called_nb and calling_nb strings and sends any IA5 character in the called_nb, and is not restricted to extended digits only (i.e., 0-9,*,#).</li> <li>▪ <b>[16384] DLCI REVERSED OPTION</b> = Behavior bit used in the IUA interface groups to indicate that the reversed format of the DLCI field must be used.</li> </ul> <p><b>Note:</b> When using the <i>ini</i> file to configure the device to support several ISDNOutCallsBehavior features, add the individual feature values. For example, to support both <b>[2]</b> and <b>[16]</b> features, set ISDNOutCallsBehavior = 18 (i.e., 2 + 16).</p>
<b>[ISDNOutCallsBehavior_x]</b>	Same as the description for parameter ISDNOutCallsBehavior, but for a specific trunk ID.
Web: ISDN NS Behaviour 2 CLI: isdn-bits-ns-extension-behavior <b>[ISDNNSBehaviour2]</b>	<p>Bit-field to determine several behavior options that influence the behavior of the Q.931 protocol.</p> <ul style="list-style-type: none"> <li>▪ <b>[8] NS BEHAVIOUR2 ANY UUI</b> = Any User to User Information Element (UUIE) is accepted for any protocol discriminator. This is useful for interoperability with non-standard switches.</li> <li>▪ <b>[16] NS BEHAVIOUR2 DISPLAY</b> = The Display IE is accepted even if it is not defined in the QSIG ISDN protocol standard. This is applicable only when configuration is QSI.</li> <li>▪ <b>[64] NS BEHAVIOUR2 FAC REJECT</b> = When this bit is set, the device answers with a Facility IE message with the Reject component on receipt of Facility IE with unknown/invalid Invoke component. This bit is implemented in QSIG and ETSI variants.</li> </ul>

Parameter	Description
<b>[PSTNExtendedParams]</b>	<p>Determines the bit map for special PSTN behavior parameters:</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Applicable for NI-2 ISDN and QSIG "Networking Extensions". This bit (i.e., bit #0) is responsible for the Invoke ID size: <ul style="list-style-type: none"> <li>✓ If this bit is not set (default), then the Invoke ID size is always one byte, with a value of 01 to 7f.</li> <li>✓ If this bit is set, then the Invoke ID size is one or two bytes according to the Invoke ID value.</li> </ul> </li> <li>▪ <b>[2]</b> = Applicable to the ROSE format (according to the old QSIG specifications). This bit (i.e., bit #1) is responsible for the QSIG octet 3. According to the ECMA-165 new version, octet 3 in all QSIG supplementary services Facility messages should be 0x9F = Networking Extensions. However, according to the old version, the value should be 0x91 = ROSE: <ul style="list-style-type: none"> <li>✓ If this bit is not set (default): 0x9F = Networking Extensions.</li> <li>✓ If this bit is set: 0x91 = ROSE.</li> </ul> </li> <li>▪ <b>[3]</b> = Use options <b>[0]</b> and <b>[2]</b> above.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>

### 59.11.7 ISDN and CAS Interworking Parameters

The ISDN and CAS interworking parameters are described in the table below.

**ISDN and CAS Interworking Parameters**

Parameter	Description
<b>ISDN Parameters</b>	
Web: Send Local Time To ISDN Connect <b>[SendLocalTimeToISDNConnect]</b>	<p>Determines the device's handling of the date and time sent in the ISDN Connect message (Date / Time IE) upon receipt of SIP 200 OK messages.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) If the SIP 200 OK includes the Date header, the device sends its value in the ISDN Connect Date / Time IE. If the 200 OK does not include this header, it does not add the Date / Time IE to the sent ISDN Connect message.</li> <li>▪ <b>[1]</b> Enable = If the SIP 200 OK includes the Date header, the device sends its value (i.e. date and time) in the ISDN Connect Date / Time IE. If the 200 OK does not include this header, the device uses its internal, local date and time for the Date / Time IE, which it adds to the sent ISDN Connect message.</li> <li>▪ <b>[2]</b> Always Send Local Date and Time = The device always sends its local date and time (obtained from its internal clock) to PBXs in ISDN Q.931 Connect messages (Date / Time IE). It does this regardless of whether or not the incoming SIP 200 OK includes the Date header. If the SIP 200 OK includes the Date header, the device ignores its value.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This feature is applicable only to Tel-to-IP calls.</li> <li>▪ For IP-to-Tel calls, this parameter is not applicable. Only if the incoming ISDN Connect message contains the Date / Time IE does</li> </ul>

Parameter	Description
	the device add the Date header to the sent SIP 200 OK message.
Web/EMS: Min Routing Overlap Digits CLI: min-dg-b4-routing <b>[MinOverlapDigitsForRouting]</b>	<p>Defines the minimum number of overlap digits to collect (for ISDN overlap dialing) before sending the first SIP message for routing Tel-to-IP calls.</p> <p>The valid value range is 0 to 49. The default is 1.</p> <p><b>Note:</b> This parameter is applicable when the ISDNRxOverlap parameter is set to <b>[2]</b>.</p>
Web/EMS: ISDN Overlap IP to Tel Dialing CLI: isdn-tx-overlap <b>[ISDNTxOverlap]</b>	<p>Enables ISDN overlap dialing for IP-to-Tel calls. This feature is part of ISDN-to-SIP overlap dialing according to RFC 3578.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>When enabled, for each received INVITE of the same dialog session, the device sends an ISDN Setup (and subsequent ISDN Info Q.931 messages) with the collected digits to the Tel side. For all subsequent INVITEs received, the device sends a SIP 484 Address Incomplete response in order to maintain the current dialog session and receive additional digits from subsequent INVITEs.</p> <p><b>Note:</b> When IP-to-Tel overlap dialing is enabled, to send ISDN Setup messages without the Sending Complete IE, the ISDNOutCallsBehavior parameter must be set to USER SENDING COMPLETE (2).</p>
Web: Enable Receiving of Overlap Dialing CLI: ovrlp-rcving-type <b>[ISDNRxOverlap_x]</b>	<p>Determines the receiving (Rx) type of ISDN overlap dialing for Tel-to-IP calls, per trunk.</p> <ul style="list-style-type: none"> <li><b>[0]</b> None = (Default) Disabled.</li> <li><b>[1]</b> Local receiving = ISDN Overlap Dialing - the complete number is sent in the INVITE Request-URI user part. The device receives ISDN called number that is sent in the 'Overlap' mode. The ISDN Setup message is sent to IP only after the number (including the Sending Complete IE) is fully received (via Setup and/or subsequent Info Q.931 messages). In other words, the device waits until it has received all the ISDN signaling messages containing parts of the called number, and only then it sends a SIP INVITE with the entire called number in the Request-URI.</li> <li><b>[2]</b> Through SIP = Interworking of ISDN Overlap Dialing to SIP, based on RFC 3578. The device interworks ISDN to SIP by sending digits each time they are received (from Setup and subsequent Info Q.931 messages) to the IP, using subsequent SIP INVITE messages.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>When option <b>[2]</b> is configured, you can define the minimum number of overlap digits to collect before sending the first SIP message for routing the call, using the MinOverlapDigitsForRouting parameter.</li> <li>When option <b>[2]</b> is configured, even if SIP 4xx responses are received during this ISDN overlap receiving, the device does not release the call.</li> <li>The MaxDigits parameter can be used to limit the length of the collected number for ISDN overlap dialing (if Sending Complete is not received).</li> <li>If a digit map pattern is defined (using the DigitMapping or DialPlanIndex parameters), the device collects digits until a match is found (e.g., for closed numbering schemes) or until a timer expires (e.g., for open numbering schemes). If a match is found (or the timer expires), the digit collection process is terminated even if Sending</li> </ul>

Parameter	Description
	<p>Complete is not received.</p> <ul style="list-style-type: none"> <li>For enabling ISDN overlap dialing for IP-to-Tel calls, use the ISDNTxOverlap parameter.</li> <li>The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.</li> <li>For more information on ISDN overlap dialing, see 'ISDN Overlap Dialing' on page 286.</li> </ul>
CLI: ovrlp-rcving-type <b>[ISDNRxOverlap]</b>	Same as the description for parameter ISDNRxOverlap_x, but for all trunks.
Web/EMS: Mute DTMF In Overlap <b>[MuteDTMFInOverlap]</b>	<p>Enables the muting of in-band DTMF detection until the device receives the complete destination number from the ISDN (for Tel-to-IP calls). In other words, the device does not accept DTMF digits received in the voice stream from the PSTN, but only accepts digits from ISDN Info messages.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Don't Mute (default).</li> <li><b>[1]</b> Mute DTMF in Overlap Dialing = The device ignores in-band DTMF digits received during ISDN overlap dialing (disables the DTMF in-band detector).</li> </ul> <p><b>Note:</b> This parameter is applicable to ISDN Overlap mode only when dialed numbers are sent using Q.931 Information messages.</p>
<b>[ConnectedNumberType]</b>	<p>Defines the Numbering Type of the ISDN Q.931 Connected Number IE that the device sends in the Connect message to the ISDN (for Tel-to-IP calls). This is interworked from the P-Asserted-Identity header in SIP 200 OK.</p> <p>The default is <b>[0]</b> (i.e., unknown).</p>
<b>[ConnectedNumberPlan]</b>	<p>Defines the Numbering Plan of the ISDN Q.931 Connected Number IE that the device sends in the Connect message to the ISDN (for Tel-to-IP calls). This is interworked from the P-Asserted-Identity header in SIP 200 OK.</p> <p>The default is <b>[0]</b> (i.e., unknown).</p>
Web/EMS: Enable ISDN Tunneling Tel to IP CLI: isdn-tnl-tel2ip <b>[EnableISDNTunnelingTel2IP]</b>	<p>Enables ISDN Tunneling.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> Using Header = Enable ISDN Tunneling from ISDN PRI to SIP using a proprietary SIP header.</li> <li><b>[2]</b> Using Body = Enable ISDN Tunneling from ISDN PRI to SIP using a dedicated message body.</li> </ul> <p>When ISDN Tunneling is enabled, the device sends all ISDN PRI messages using the correlated SIP messages. The ISDN Setup message is tunneled using SIP INVITE, all mid-call messages are tunneled using SIP INFO, and ISDN Disconnect/Release message is tunneled using SIP BYE messages. The raw data from the ISDN is inserted into a proprietary SIP header (X-ISDNTunnelingInfo) or a dedicated message body (application/isdn) in the SIP messages.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this feature to function, you must set the parameter ISDNDuplicateQ931BuffMode to 128 (i.e., duplicate all messages).</li> <li>ISDN tunneling is applicable for all ISDN variants as well as QSIG.</li> </ul>
Web/EMS: Enable ISDN Tunneling IP to Tel CLI: isdn-tnl-ip2tel	<p>Enables ISDN Tunneling for IP-to-Tel calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> </ul>

Parameter	Description
<b>[EnableISDNTunneling]</b> <b>P2Tel]</b>	<ul style="list-style-type: none"> <li><b>[1]</b> Enable ISDN Tunneling from IP to ISDN</li> </ul> <p>When ISDN Tunneling is enabled, the device extracts raw data received in the proprietary SIP header, x-isdntunnelinginfo, or a dedicated message body (application/isdn) in the SIP message and then sends the data in an ISDN message to the PSTN.</p> <p>If the raw data in this SIP header is suffixed with the string "ADDE", then the raw data is extracted and added as Informational Elements (IE) in the outgoing Q.931 message. The tunneling of the x-isdntunnelinginfo SIP header with IEs is converted from INVITE, 180, and 200 OK SIP messages to Q.931 SETUP, ALERT, and CONNECT respectively.</p> <p>For example, if the following SIP header is received,</p> <pre>x-isdntunnelinginfo: ADDE1C269FAA 06 800100820100A10F020136 0201F0A00702010102021F69</pre> <p>then it is added as an IE to the outgoing Q.931 message as 1C269FAA 06 800100820100A10F020136 0201F0A00702010102021F69, where, for example, "1C269F" is a 26 byte length Facility IE.</p> <p><b>Note:</b> This feature is similar to that of the AddIEinSetup parameter. If both parameters are configured, the x-isdntunneling parameter takes precedence.</p>
Web/EMS: Enable QSIG Tunneling CLI: qsig-tunneling <b>[EnableQSIGTunneling]</b>	<p>Enables QSIG tunneling-over-SIP for all calls. This is according to IETF Internet-Draft draft-elwell-sipping-qsig-tunnel-03 and ECMA-355 and ETSI TS 102 345.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> Enable = Enable QSIG tunneling from QSIG to SIP and vice versa. All QSIG messages are sent as raw data in corresponding SIP messages using a dedicated message body.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This feature can also be configured in an IP Profile.</li> <li>QSIG tunneling must be enabled on originating and terminating devices.</li> <li>To enable this function, set the ISDNDuplicateQ931BuffMode parameter to 128 (i.e., duplicate all messages).</li> <li>To define the format of encapsulated QSIG messages, use the QSIGTunnelingMode parameter.</li> <li>Tunneling according to ECMA-355 is applicable to all ISDN variants (in addition to the QSIG protocol).</li> <li>For more information on QSIG tunneling, see 'QSIG Tunneling' on page 282.</li> </ul>
<b>[QSIGTunnelingMode]</b>	<p>Defines the format of encapsulated QSIG message data in the SIP message MIME body.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) ASCII presentation of Q.931 QSIG message.</li> <li><b>[1]</b> = Binary encoding of Q.931 QSIG message (according to ECMA-355, RFC 3204, and RFC 2025).</li> </ul> <p><b>Note:</b> This parameter is applicable only if the QSIG Tunneling feature is enabled (using the EnableQSIGTunneling parameter).</p>
Web: Enable Hold to ISDN EMS: Enable Hold 2 ISDN CLI: hold-to-isdn <b>[EnableHold2ISDN]</b>	<p>Enables SIP-to-ISDN interworking of the Hold/Retrieve supplementary service.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable to Euro ISDN variants - from TE (user)</li> </ul>



Parameter	Description
	<p>to NT (network).</p> <ul style="list-style-type: none"> <li>This parameter is applicable also to QSIG BRI.</li> <li>If the parameter is disabled, the device plays a held tone to the Tel side when a SIP request with 0.0.0.0 or "inactive" in SDP is received. An appropriate CPT file with the held tone should be used.</li> </ul>
EMS: Duplicate Q931 Buff Mode [ISDNDuplicateQ931BuffMode]	<p>Determines the activation/deactivation of delivering raw Q.931 messages.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) ISDN messages aren't duplicated.</li> <li><b>[128]</b> = All ISDN messages are duplicated.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web/EMS: ISDN SubAddress Format CLI: isdn-subaddr-frmt [ISDNSubAddressFormat]	<p>Determines the encoding format of the SIP Tel URI parameter 'isub', which carries the encoding type of ISDN subaddresses. This is used to identify different remote ISDN entities under the same phone number (ISDN Calling and Called numbers) for interworking between ISDN and SIP networks.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) ASCII - IA5 format that allows up to 20 digits. Indicates that the 'isub' parameter value needs to be encoded using ASCII characters.</li> <li><b>[1]</b> = BCD (Binary Coded Decimal) - allows up to 40 characters (digits and letters). Indicates that the 'isub' parameter value needs to be encoded using BCD when translated to an ISDN message.</li> <li><b>[2]</b> = User Specified</li> </ul> <p>For IP-to-Tel calls, if the incoming SIP INVITE message includes subaddress values in the 'isub' parameter for the Called Number (in the Request-URI) and/or the Calling Number (in the From header), these values are mapped to the outgoing ISDN Setup message.</p> <p>If the incoming ISDN Setup message includes 'subaddress' values for the Called Number and/or the Calling Number, these values are mapped to the outgoing SIP INVITE message's 'isub' parameter in accordance with RFC 4715.</p>
[IgnoreISDNSubaddresses]	<p>Determines whether the device ignores the Subaddress from the incoming ISDN Called and Calling numbers when sending to IP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) If an incoming ISDN Q.931 Setup message contains a Called/Calling Number Subaddress, the Subaddress is interworked to the SIP 'isub' parameter according to RFC.</li> <li><b>[1]</b> = The device removes the ISDN Subaddress and does not include the 'isub' parameter in the Request-URI and does not process INVITEs with this parameter.</li> </ul>
[ISUBNumberOfDigits]	<p>Defines the number of digits (from the end) that the device takes from the called number (received from the IP) for the isub number (in the sent ISDN Setup message). This feature is only applicable for IP-to-ISDN calls.</p> <p>The valid value range is 0 to 36. The default is 0.</p> <p>This feature operates as follows:</p> <ol style="list-style-type: none"> <li>If an isub parameter is received in the Request-URI, for example, INVITE sip:9565645;<b>isub</b>=1234@host.domain:user=phone SIP/2.0 then the isub value is sent in the ISDN Setup message as the destination subaddress.</li> <li>If the isub parameter is not received in the user part of the Request-URI, the device searches for it in the URI parameters of the To</li> </ol>

Parameter	Description
	<p>header, for example, To: "Alex" &lt;sip: 9565645@host.domain;<b>isub</b>=1234&gt; If present, the isub value is sent in the ISDN Setup message as the destination subaddress.</p> <p><b>3</b> If the isub parameter is not present in the Request-URI header nor To header, the device does the following:</p> <ul style="list-style-type: none"> <li>✓ If the called number (that appears in the user part of the Request-URI) starts with zero (0), for example, INVITE sip:05694564@host.domain:user=phone SIP/2.0 then the device maps this called number to the destination number of the ISDN Setup message, and the destination subaddress in this ISDN Setup message remains empty.</li> <li>✓ If the called number (that appears in the user part of the Request-URI) does not start with zero, for example, INVITE sip:5694564@host.domain:user=phone SIP/2.0 then the device maps this called number to the destination number of the ISDN Setup message, and the destination subaddress in this ISDN Setup message then contains y digits from the end of the called number. The y number of digits can be configured using the ISUBNumberOfDigits parameter. The default value of ISUBNumberOfDigits is 0, thus, if this parameter is not configured, and 1) and 2) scenarios (described above) have not provided an isub value, the subaddress remains empty.</li> </ul>
Web: Default Cause Mapping From ISDN to SIP CLI: dflt-cse-map-isdn2sip <b>[DefaultCauseMapISDN2IP]</b>	Defines a single default ISDN release cause that is used (in ISDN-to-IP calls) instead of all received release causes, except when the following Q.931 cause values are received: Normal Call Clearing (16), User Busy (17), No User Responding (18), or No Answer from User (19). The range is any valid Q.931 release cause (0 to 127). The default is 0 (i.e., not configured - static mapping is used).
<b>Release Cause Mapping from ISDN to SIP Table</b>	
Web: Release Cause Mapping Table EMS: ISDN to SIP Cause Mapping CLI: configure voip > gw manipulations CauseMapIsdn2Sip <b>[CauseMapISDN2SIP]</b>	<p>This table parameter maps ISDN Q.850 Release Causes to SIP responses.  The format of this parameter is as follows:  <b>[CauseMapISDN2SIP]</b>  FORMAT CauseMapISDN2SIP_Index = CauseMapISDN2SIP_IsdnReleaseCause, CauseMapISDN2SIP_SipResponse;  <b>[CauseMapISDN2SIP]</b></p> <p>Where,</p> <ul style="list-style-type: none"> <li>IsdnReleaseCause = Q.850 Release Cause</li> <li>SipResponse = SIP Response</li> </ul> <p>For example:  CauseMapISDN2SIP 0 = 50,480;  CauseMapISDN2SIP 0 = 6,406;</p> <p>When a Release Cause is received (from the PSTN side), the device searches this mapping table for a match. If the Q.850 Release Cause is found, the SIP response assigned to it is sent to the IP side. If no match is found, the default static mapping is used.</p> <p><b>Note:</b> This parameter can appear up to 12 times.</p>
<b>Release Cause Mapping from SIP to ISDN Table</b>	
Web: Release Cause	This table parameter maps SIP responses to Q.850 Release Causes.



Parameter	Description
Mapping Table EMS: SIP to ISDN Cause Mapping CLI: configure voip > gw manipulations CauseMapSip2Isdn <b>[CauseMapSIP2ISDN]</b>	<p>The format of this parameter is as follows:  <b>[CauseMapSIP2ISDN]</b>            FORMAT CauseMapSIP2ISDN_Index =            CauseMapSIP2ISDN_SipResponse,            CauseMapSIP2ISDN_IsdnReleaseCause;  <b>[CauseMapSIP2ISDN]</b></p> <p>Where,</p> <ul style="list-style-type: none"> <li>SipResponse = SIP Response</li> <li>IsdnReleaseCause = Q.850 Release Cause</li> </ul> <p>For example:            CauseMapSIP2ISDN 0 = 480,50;            CauseMapSIP2ISDN 0 = 404,3;            When a SIP response is received (from the IP side), the device searches this mapping table for a match. If the SIP response is found, the Q.850 Release Cause assigned to it is sent to the PSTN. If no match is found, the default static mapping is used.</p> <p><b>Note:</b> This parameter can appear up to 12 times.</p>
Web/EMS: Enable Calling Party Category CLI: ni2-cpc <b>[EnableCallingPartyCategory]</b>	<p>Determines whether Calling Party Category (CPC) is mapped between SIP and PRI.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Don't relay the CPC between SIP and PRI.</li> <li><b>[1]</b> Enable = The CPC is relayed between SIP and PRI.</li> </ul> <p>If enabled, the CPC received in the Originating Line Information (OLI) IE of an incoming ISDN Setup message is relayed to the From/P-Asserted-Identity headers using the 'cpc' parameter in the outgoing INVITE message, and vice versa.</p> <p>For example (calling party is a payphone):</p> <pre>From:&lt;sip:2000;cpc=payphone@10.8.23.70&gt;;tag=1c1806157451</pre> <p><b>Note:</b> This feature is applicable only to the NI-2 PRI variant.</p>
CLI: usr2usr-hdr-frmt <b>[UserToUserHeaderFormat]</b>	<p>Defines the interworking between the SIP INVITE's User-to-User header and the ISDN User-to-User (UU) IE data.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) SIP header format: X-UserToUser.</li> <li><b>[1]</b> = SIP header format: User-to-User with Protocol Discriminator (pd) attribute (according to IETF Internet-Draft draft-johnston-sipping-cc-uui-04). For example:  <pre>User-to-User=3030373435313734313635353b313233343b3834;pd=4</pre></li> <li><b>[2]</b> = SIP header format: User-to-User with encoding=hex at the end and pd embedded as the first byte (according to IETF Internet-Draft draft-johnston-sipping-cc-uui-03). For example:  <pre>User-to-User=043030373435313734313635353b313233343b3834;encoding=hex</pre> <p>where "04" at the beginning of this message is the pd.</p></li> <li><b>[3]</b> = Interworks the SIP User-to-User header containing text format to ISDN UUIE in hexadecimal format, and vice versa. For example:            SIP Header in text format:  <pre>User-to-User=01800213027b712a;NULL;4582166;</pre> <p>Translated to hexadecimal in the ISDN UUIE:            303138303032313330323762373132613b4e554c4c3b3435383</p></li> </ul>

Parameter	Description
	<p>23136363b</p> <p>The Protocol Discriminator (pd) used in UUIE is "04" (IUA characters).</p> <p><b>Note:</b> This parameter is applicable for Tel-to-IP and IP-to-Tel calls.</p>
Web/EMS: Remove CLI when Restricted CLI: rmv-cli-when-restr <b>[RemoveCLIWhenRestricted]</b>	<p>Determines (for IP-to-Tel calls) whether the Calling Number and Calling Name IEs are removed from the ISDN Setup message if the presentation is set to Restricted.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) IE's are not removed.</li> <li><b>[1]</b> Yes = IE's are removed.</li> </ul>
Web/EMS: Remove Calling Name CLI: rmv-calling-name <b>[RemoveCallingName]</b>	<p>Enables the device to remove the Calling Name from SIP-to-ISDN calls for all trunks.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Does not remove Calling Name.</li> <li><b>[1]</b> Enable = Removes Calling Name.</li> </ul> <p><b>Note:</b> Some PSTN switches / PBXs may not be configured to support the receipt of the "Calling Name" information. These switches might respond to an ISDN Setup message (including the Calling Name) with an ISDN "REQUESTED_FAC_NOT_SUBSCRIBED" failure. This parameter can be set to Enable (1) to remove the "Calling Name" from SIP-to-ISDN calls and allow the call to proceed.</p>
Web: Remove Calling Name EMS: Remove Calling Name For Trunk Mode <b>[RemoveCallingNameForTrunk_x]</b>	<p>Enables the device to remove the Calling Name for SIP-to-ISDN calls, per trunk.</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Use Global Parameter = (Default) Settings of the global parameter RemoveCallingName are used.</li> <li><b>[0]</b> Disable = Does not remove Calling Name.</li> <li><b>[1]</b> Enable = Remove Calling Name.</li> </ul> <p><b>Note:</b> The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1</p>
Web/EMS: Progress Indicator to ISDN CLI: pi-to-isdn <b>[ProgressIndicator2ISDN_x]</b>	<p>Determines the Progress Indicator (PI) to ISDN, per trunk.</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured = (Default) The PI in ISDN messages is set according to the parameter PlayRBTone2Tel.</li> <li><b>[0]</b> No PI = PI is not sent to ISDN.</li> <li><b>[1]</b> PI = 1; <b>[8]</b> PI = 8: The PI value is sent to PSTN in Q.931/Proceeding and Alerting messages. Typically, the PSTN/PBX cuts through the audio channel without playing local ringback tone, enabling the originating party to hear remote Call Progress Tones or network announcements.</li> </ul> <p><b>Note:</b> The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.</p>
Web: Set PI in Rx Disconnect Message EMS: Set PI For Disconnect Msg CLI: pi-in-rx-disc-msg <b>[PIForDisconnectMsg_x]</b>	<p>Defines the device's behavior per trunk when a Disconnect message is received from the ISDN before a Connect message is received.</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured = (Default) Sends a 183 SIP response according to the received progress indicator (PI) in the ISDN Disconnect message. If PI = 1 or 8, the device sends a 183 response, enabling the PSTN to play a voice announcement to the IP side. If there isn't a PI in the Disconnect message, the call is released.</li> <li><b>[0]</b> No PI = Doesn't send a 183 response to IP. The call is released.</li> <li><b>[1]</b> PI = 1; <b>[8]</b> PI = 8: Sends a 183 response to IP.</li> </ul> <p><b>Note:</b> The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.</p>
EMS: Connect On	Enables the play of announcements from IP to PSTN without the need

Parameter	Description
Progress Ind [ConnectOnProgressInd]	to answer the Tel-to-IP call. It can be used with PSTN networks that don't support the opening of a TDM channel before an ISDN Connect message is received. <ul style="list-style-type: none"> <li>[0] = (Default) Connect message isn't sent after SIP 183 Session Progress message is received.</li> <li>[1] = Connect message is sent after SIP 183 Session Progress message is received.</li> </ul>
Web: Local ISDN Ringback Tone Source EMS: Local ISDN RB Source CLI: local-isdn-rbt-src [LocalISDNRBSource_x]	Determines whether the ringback tone is played to the ISDN by the PBX/PSTN or by the device, per trunk. <ul style="list-style-type: none"> <li>[0] PBX = (Default) PBX/PSTN.</li> <li>[1] Gateway = The device plays the ringback tone.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable to ISDN protocols.</li> <li>This parameter is used together with the parameter PlayRBTone2Trunk.</li> <li>The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.</li> </ul>
Web/EMS: PSTN Alert Timeout CLI: pstn-alrt-timeout [TrunkPSTNAlertTimeout_x]	Defines the Alert Timeout (ISDN T301 timer) in seconds for outgoing calls to PSTN, per trunk. This timer is used between the time that an ISDN Setup message is sent to the Tel side (IP-to-Tel call establishment) and a Connect message is received. If Alerting is received, the timer is restarted. The range is 1 to 600. The default is 180. <b>Note:</b> The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.
Web: B-Channel Negotiation EMS: B-Channel Negotiation For Trunk Mode [BChannelNegotiationForTrunk_x]	Determines the ISDN B-channel negotiation mode, per trunk. <ul style="list-style-type: none"> <li>[-1] Not Configured = (Default) Use per device configuration of the BChannelNegotiation parameter.</li> <li>[0] Preferred.</li> <li>[1] Exclusive.</li> <li>[2] Any.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable to ISDN protocols.</li> <li>The option 'Any' is only applicable if TerminationSide is set to 0 (i.e., User side).</li> <li>The x in the ini file parameter name denotes the trunk number, where 0 is the first trunk.</li> </ul>
CLI: snd-isdn-ser-aft-restart [SendISDNServiceAfterRestart]	Enables the device to send an ISDN SERVICE message per trunk upon device reset. The message (transmitted on the trunk's D-channel) indicates the availability of the trunk's B-channels (i.e., trunk in service). <ul style="list-style-type: none"> <li>[0] = Disable (default)</li> <li>[1] = Enable</li> </ul>
EMS: Support Redirect InFacility [SupportRedirectInFacility]	Determines whether the Redirect Number is retrieved from the Facility IE. <ul style="list-style-type: none"> <li>[0] = (Default) Not supported.</li> <li>[1] = Supports partial retrieval of Redirect Number (number only) from the Facility IE in ISDN Setup messages. This is applicable to Redirect Number according to ECMA-173 Call Diversion Supplementary Services.</li> </ul>

Parameter	Description
	<p><b>Note:</b> To enable this feature, the parameter ISDNDuplicateQ931BuffMode must be set to 1.</p>
CLI: call-re-rte-mode <b>[CallReroutingMode]</b>	<p>Determines whether ISDN call rerouting (call forward) is performed by the PSTN instead of by the SIP side. This call forwarding is based on Call Deflection for Euro ISDN (ETS-300-207-1) and QSIG (ETSI TS 102 393).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default).</li> <li>▪ <b>[1]</b> Enable = Enables ISDN call rerouting. When the device sends the INVITE message to the remote SIP entity and receives a SIP 302 response with a Contact header containing a URI host name that is the same as the device's IP address, the device sends a Facility message with a Call Rerouting invoke method to the ISDN and waits for the PSTN side to disconnect the call.</li> </ul> <p><b>Note:</b> When this parameter is enabled, ensure that you configure in the Inbound IP Routing Table (PSTNPrefix <i>ini</i> file parameter) a rule to route the redirected call (using the user part from the 302 Contact header) to the same Trunk Group from where the incoming Tel-to-IP call was received.</p>
EMS: Enable CIC <b>[EnableCIC]</b>	<p>Determines whether the Carrier Identification Code (CIC) is relayed to ISDN.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Do not relay the Carrier Identification Code (CIC) to ISDN.</li> <li>▪ <b>[1]</b> = CIC is relayed to the ISDN in Transit Network Selection (TNS) IE.</li> </ul> <p>If enabled, the CIC code (received in an INVITE Request-URI) is included in a TNS IE in the ISDN Setup message.            For example: INVITE sip:5556666;cic=2345@100.2.3.4 sip/2.0.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This feature is supported only for SIP-to-ISDN calls.</li> <li>▪ The parameter AddCicAsPrefix can be used to add the CIC as a prefix to the destination phone number for routing IP-to-Tel calls.</li> </ul>
EMS: Enable AOC <b>[EnableAOC]</b>	<p>Determines whether ISDN Advice of Charge (AOC) messages are interworked with SIP.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Not used.</li> <li>▪ <b>[1]</b> = AOC messages are interworked to SIP (in receive direction) and sent to the PSTN in the transmit direction.</li> </ul> <p>The device supports both the receipt and sending of ISDN (Euro ISDN) AOC messages:</p> <ul style="list-style-type: none"> <li>▪ AOC messages can be received during a call (Facility messages) or at the end of a call (Disconnect or Release messages). The device converts the AOC messages into SIP INFO (during a call) and BYE (end of a call) messages, using a proprietary AOC SIP header. The device supports both Currency and Pulse AOC messages.</li> <li>▪ AOC messages can be sent during a call (Facility messages) or at the end of a call (Disconnect or Release messages). This is done by assigning the Charge Code index to the desired routing rule in the Outbound IP Routing table. For more information, see 'Advice of Charge Services for Euro ISDN' on page 388.</li> </ul>
Web: IPMedia Detectors EMS: DSP Detectors Enable CLI: IPM-detectors-	<p>Enables the device's DSP detectors.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul>

Parameter	Description
enable [EnableDSIPMDetectors]	<b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>The device's Software License Key must contain the 'IPMDetector' DSP option.</li> <li>When enabled (1), the number of available channels is reduced.</li> </ul>
Web: Add IE in SETUP EMS: IE To Be Added In Q.931 Setup CLI: add-ie-in-setup [AddIEinSetup]	<p>Adds an optional Information Element (IE) data (in hex format) to ISDN Setup messages. For example, to add IE '0x20,0x02,0x00,0xe1', enter the value "200200e1".</p> <b>Notes:</b> <ul style="list-style-type: none"> <li>This IE is sent from the Trunk Group IDs that are defined by the parameter SendIEonTG.</li> <li>You can configure different IE data for Trunk Groups by defining this parameter for different IP Profiles (using the IPProfile parameter) and then assigning the required IP Profile ID in the Inbound IP Routing Table (PSTNPrefix).</li> <li>This feature is similar to that of the EnableISDNTunnelingIP2Tel parameter. If both parameters are configured, the EnableISDNTunnelingIP2Tel parameter takes precedence.</li> </ul>
Web: Trunk Groups to Send IE EMS: List Of Trunk Groups To Send IE CLI: trkgtps-to-snd-ie [SendIEonTG]	<p>Defines Trunk Group IDs (up to 50 characters) from where the optional ISDN IE (defined by the parameter AddIEinSetup) is sent. For example: '1,2,4,10,12,6'.</p> <b>Notes:</b> <ul style="list-style-type: none"> <li>You can configure different IE data for Trunk Groups by defining this parameter for different IP Profile IDs (using the parameter IPProfile), and then assigning the required IP Profile ID in the Inbound IP Routing Table (PSTNPrefix).</li> <li>When IP Profiles are used for configuring different IE data for Trunk Groups, this parameter is ignored.</li> </ul>
Web: Enable User-to-User IE for Tel to IP EMS: Enable UUI Tel 2 Ip CLI: uui-ie-for-tel2ip [EnableUUITel2IP]	<p>Enables transfer of User-to-User (UU) IE from ISDN PRI to SIP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>The device supports the following ISDN PRI-to-SIP interworking: Setup to SIP INVITE, Connect to SIP 200 OK, User Information to SIP INFO, Alerting to SIP 18x response, and Disconnect to SIP BYE response messages.</p> <p><b>Note:</b> The interworking of ISDN User-to-User IE to SIP INFO is applicable only to the Euro ISDN, QSIG, and 4ESS PRI variants.</p>
Web: Enable User-to-User IE for IP to Tel EMS: Enable UUI Ip 2 Tel CLI: uui-ie-for-ip2tel [EnableUUIIP2Tel]	<p>Enables interworking of SIP user-to-user information (UUI) to User-to-User IE in ISDN Q.931 messages.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Received UUI is not sent in ISDN message.</li> <li><b>[1]</b> Enable = The device interworks UUI from SIP to ISDN messages. The device supports the following SIP-to-ISDN interworking of UUI: <ul style="list-style-type: none"> <li>✓ SIP INVITE to Q.931 Setup</li> <li>✓ SIP REFER to Q.931 Setup</li> <li>✓ SIP 200 OK to Q.931 Connect</li> <li>✓ SIP INFO to Q.931 User Information</li> <li>✓ SIP 18x to Q.931 Alerting</li> <li>✓ SIP BYE to Q.931 Disconnect</li> </ul> </li> </ul> <b>Notes:</b>

Parameter	Description														
	<ul style="list-style-type: none"> <li>The interworking of ISDN User-to-User IE to SIP INFO is applicable only to the Euro ISDN, QSIG, and 4ESS PRI variants.</li> <li>To interwork the UUIE header from SIP-to-ISDN messages with the 4ESS ISDN variant, the ISDNGeneralCCBehavior parameter must be set to 16384.</li> </ul>														
<b>[Enable911LocationIdl P2Tel]</b>	<p>Enables interworking of Emergency Location Identification from SIP to PRI.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disabled (default)</li> <li><b>[1]</b> = Enabled</li> </ul> <p>When enabled, the From header received in the SIP INVITE is translated into the following ISDN IE's:</p> <ul style="list-style-type: none"> <li>Emergency Call Control.</li> <li>Generic Information - to carry the Location Identification Number information.</li> <li>Generic Information - to carry the Calling Geodetic Location information.</li> </ul> <p><b>Note:</b> This capability is applicable only to the NI-2 ISDN variant.</p>														
CLI: early-answer-timeout <b>[EarlyAnswerTimeout]</b>	<p>Defines the duration (in seconds) that the device waits for an ISDN Connect message from the called party (Tel side), started from when it sends a Setup message. If this timer expires, the call is answered by sending a SIP 200 OK message (to the IP side).</p> <p>The valid range is 0 to 2400. The default is 0 (i.e., disabled).</p> <p><b>Note:</b> This parameter can be configured per IP Profile.</p>														
Web/EMS: Trunk Transfer Mode CLI: trk-xfer-mode-type <b>[TrunkTransferMode]</b>	<p>Determines the trunk transfer method (for all trunks) when a SIP REFER message is received. The transfer method depends on the Trunk's PSTN protocol (configured by the parameter ProtocolType) and is applicable only when one of these protocols are used:</p> <table border="1"> <thead> <tr> <th>PSTN Protocol</th><th>Transfer Method (Described Below)</th></tr> </thead> <tbody> <tr> <td>E1 Euro ISDN <b>[1]</b></td><td>ECT <b>[2]</b> or InBand <b>[5]</b></td></tr> <tr> <td>E1 QSIG <b>[21]</b>, T1 QSIG <b>[23]</b></td><td>Single Step Transfer <b>[4]</b>, Path Replacement Transfer <b>[2]</b>, or InBand <b>[5]</b></td></tr> <tr> <td>T1 NI2 ISDN <b>[10]</b>, T1 4ESS ISDN <b>[11]</b>, T1 5ESS 9 ISDN <b>[12]</b></td><td>TBCT <b>[2]</b> or InBand <b>[5]</b></td></tr> <tr> <td>T1 DMS-100 ISDN <b>[14]</b></td><td>RTL <b>[2]</b> or InBand <b>[5]</b></td></tr> <tr> <td>T1 RAW CAS <b>[3]</b>, T1 CAS <b>[2]</b>, E1 CAS <b>[8]</b>, E1 RAW CAS <b>[9]</b></td><td><b>[1]</b> CAS NFA DMS-100 or <b>[3]</b> CAS Normal transfer</td></tr> <tr> <td>T1 DMS-100 Meridian ISDN <b>[35]</b></td><td>RTL <b>[2]</b> or InBand <b>[5]</b></td></tr> </tbody> </table> <p>The valid values of this parameter are described below:</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Not supported (default).</li> <li><b>[1]</b> = Supports CAS NFA DMS-100 transfer. When a SIP REFER message is received, the device performs a Blind Transfer by executing a CAS Wink, waits for an acknowledged Wink from the remote side, dials the Refer-to number to the switch, and then releases the call.</li> </ul>	PSTN Protocol	Transfer Method (Described Below)	E1 Euro ISDN <b>[1]</b>	ECT <b>[2]</b> or InBand <b>[5]</b>	E1 QSIG <b>[21]</b> , T1 QSIG <b>[23]</b>	Single Step Transfer <b>[4]</b> , Path Replacement Transfer <b>[2]</b> , or InBand <b>[5]</b>	T1 NI2 ISDN <b>[10]</b> , T1 4ESS ISDN <b>[11]</b> , T1 5ESS 9 ISDN <b>[12]</b>	TBCT <b>[2]</b> or InBand <b>[5]</b>	T1 DMS-100 ISDN <b>[14]</b>	RTL <b>[2]</b> or InBand <b>[5]</b>	T1 RAW CAS <b>[3]</b> , T1 CAS <b>[2]</b> , E1 CAS <b>[8]</b> , E1 RAW CAS <b>[9]</b>	<b>[1]</b> CAS NFA DMS-100 or <b>[3]</b> CAS Normal transfer	T1 DMS-100 Meridian ISDN <b>[35]</b>	RTL <b>[2]</b> or InBand <b>[5]</b>
PSTN Protocol	Transfer Method (Described Below)														
E1 Euro ISDN <b>[1]</b>	ECT <b>[2]</b> or InBand <b>[5]</b>														
E1 QSIG <b>[21]</b> , T1 QSIG <b>[23]</b>	Single Step Transfer <b>[4]</b> , Path Replacement Transfer <b>[2]</b> , or InBand <b>[5]</b>														
T1 NI2 ISDN <b>[10]</b> , T1 4ESS ISDN <b>[11]</b> , T1 5ESS 9 ISDN <b>[12]</b>	TBCT <b>[2]</b> or InBand <b>[5]</b>														
T1 DMS-100 ISDN <b>[14]</b>	RTL <b>[2]</b> or InBand <b>[5]</b>														
T1 RAW CAS <b>[3]</b> , T1 CAS <b>[2]</b> , E1 CAS <b>[8]</b> , E1 RAW CAS <b>[9]</b>	<b>[1]</b> CAS NFA DMS-100 or <b>[3]</b> CAS Normal transfer														
T1 DMS-100 Meridian ISDN <b>[35]</b>	RTL <b>[2]</b> or InBand <b>[5]</b>														



Parameter	Description
	<p><b>Note:</b> A specific NFA CAS table is required.</p> <ul style="list-style-type: none"> <li>▪ <b>[2]</b> = Supports ISDN (PRI/BRI) transfer - Release Link Trunk (RLT) (DMS-100), Two B Channel Transfer (TBCT) (NI2), Explicit Call Transfer (ECT) (EURO ISDN), and Path Replacement (QSIG). When a SIP REFER message is received, the device performs a transfer by sending Facility messages to the PBX with the necessary information on the call's legs to be connected. The different ISDN variants use slightly different methods (using Facility messages) to perform the transfer.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>✓ For RLT ISDN transfer, the parameter <code>SendISDNTransferOnConnect</code> must be set to 1.</li> <li>✓ The parameter <code>SendISDNTransferOnConnect</code> can be used to define if the TBCT/ECT transfer is performed after receipt of Alerting or Connect messages. For RLT, the transfer is always done after receipt of Connect (<code>SendISDNTransferOnConnect</code> is set to 1).</li> <li>✓ This transfer can be performed between B-channels from different trunks or Trunk Groups, by using the parameter <code>EnableTransferAcrossTrunkGroups</code>.</li> <li>✓ The device initiates the ECT process after receiving a SIP REFER message only for trunks that are configured to User side.</li> </ul> <ul style="list-style-type: none"> <li>▪ <b>[3]</b> = Supports CAS Normal transfer. When a SIP REFER message is received, the device performs a Blind Transfer by executing a CAS Wink, dialing the Refer-to number to the switch, and then releasing the call.</li> <li>▪ <b>[4]</b> = Supports QSIG Single Step transfer (PRI/BRI):  IP-to-Tel: When a SIP REFER message is received, the device performs a transfer by sending a Facility message to the PBX, initiating Single Step transfer. Once a success return result is received, the transfer is completed.  Tel-to-IP: When a Facility message initiating Single Step transfer is received from the PBX, a SIP REFER message is sent to the IP side.</li> <li>▪ <b>[5]</b> = IP-to-Tel Blind Transfer mode supported for ISDN (PRI/BRI) protocols and implemented according to AT&amp;T Toll Free Transfer Connect Service (TR 50075) "Courtesy Transfer-Human-No Data". When the device receives a SIP REFER message, it performs a blind transfer by first dialing the DTMF digits (transfer prefix) defined by the parameter <code>XferPrefixIP2Tel</code> (configured to "*8" for AT&amp;T service), and then (after 500 msec) the device dials the DTMF of the number (referred) from the Refer-To header sip:URI userpart. If the hostpart of the Refer-To sip:URI contains the device's IP address, and if the Trunk Group selected according to the IP to Tel Routing table is the same Trunk Group as the original call, then the device performs the in-band DTMF transfer; otherwise, the device sends the INVITE according to regular transfer rules. After completing the in-band transfer, the device waits for the ISDN Disconnect message. If the Disconnect message is received during the first 5 seconds, the device sends a SIP NOTIFY with 200 OK message; otherwise, the device sends a NOTIFY with 4xx message.</li> </ul> <p><b>Note:</b> For configuring trunk transfer mode per trunk, use the parameter <code>TrunkTransferMode_x</code>.</p>

Parameter	Description
<b>[TrunkTransferMode_x]</b>	Determines the trunk transfer mode per trunk (where x is the Trunk ID). For configuring trunk transfer mode for all trunks and for a description of the parameter options, refer to the parameter TrunkTransferMode.
<b>[EnableTransferAcrossTrunkGroups]</b>	<p>Determines whether the device allows ISDN ECT, RLT or TBCT IP-to-Tel call transfers between B-channels of different Trunk Groups.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disable - ISDN call transfer is only between B-channels of the same Trunk Group.</li> <li><b>[1]</b> = Enable - the device performs ISDN transfer between any two PSTN calls (between any Trunk Group) handled by the device.</li> </ul> <p><b>Note:</b> The ISDN transfer also requires that you configure the parameter TrunkTransferMode_x to 2.</p>
Web: ISDN Transfer Capabilities EMS: Transfer Capability To ISDN CLI: isdn-xfer-cab <b>[ISDNTransferCapability_x]</b>	<p>Defines the IP-to-ISDN Transfer Capability of the Bearer Capability IE in ISDN Setup messages, per trunk.</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured</li> <li><b>[0]</b> Audio 3.1 (default)</li> <li><b>[1]</b> Speech</li> <li><b>[2]</b> Data</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If this parameter is not configured or is set to -1, Audio 3.1 capability is used.</li> <li>The Audio 7 option is currently not supported.</li> <li>The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.</li> </ul>
<b>[TransferCapabilityForDataCalls]</b>	<p>Defines the ISDN Transfer Capability for data calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) ISDN Transfer Capability for data calls is 64k unrestricted (data).</li> <li><b>[1]</b> = ISDN Transfer Capability for data calls is determined according to the ISDNTransferCapability parameter.</li> </ul>
Web: ISDN Transfer On Connect EMS: Send ISDN Transfer On Connect CLI: isdn-trsfr-on-conn <b>[SendISDNTransferOnConnect]</b>	<p>This parameter is used for the ECT/TBCT/RLT/Path Replacement ISDN transfer methods. Usually, the device requests the PBX to connect an incoming and outgoing call. This parameter determines if the outgoing call (from the device to the PBX) must be connected before the transfer is initiated.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Alert = (Default) Enables ISDN Transfer if the outgoing call is in Alerting or Connect state.</li> <li><b>[1]</b> Connect = Enables ISDN Transfer only if the outgoing call is in Connect state.</li> </ul> <p><b>Note:</b> For RLT ISDN transfer (TrunkTransferMode = 2 and ProtocolType = 14 DMS-100), this parameter must be set to 1.</p>
<b>[ISDNTransferCompleteTimeout]</b>	<p>Defines the timeout (in seconds) for determining ISDN call transfer (ECT, RLT, or TBCT) failure. If the device does not receive any response to an ISDN transfer attempt within this user-defined time, the device identifies this as an ISDN transfer failure and subsequently performs a hairpin TDM connection or sends a SIP NOTIFY message with a SIP 603 response (depending whether hairpin is enabled or disabled, using the parameter DisableFallbackTransferToTDM). The valid range is 1 to 10. The default is 4.</p>
Web/EMS: Enable Network ISDN Transfer CLI: network-isdn-xfer	Determines whether the device allows interworking of network-side received ECT/TBCT Facility messages (NI2 TBCT - Two B-channel Transfer and ETSI ECT - Explicit Call Transfer) to SIP REFER.



Parameter	Description
<b>[EnableNetworkISDNTransfer]</b>	<ul style="list-style-type: none"> <li><b>[0]</b> Disable = Rejects ISDN transfer requests.</li> <li><b>[1]</b> Enable = (Default) The device sends a SIP REFER message to the remote call party if ECT/TBCT Facility messages are received from the ISDN side (e.g., from a PBX).</li> </ul>
<b>[DisableFallbackTransferToTDM]</b>	<p>Enables "hairpin" TDM transfer upon ISDN (ECT, RLT, or TBCT) call transfer failure. When this feature is enabled and an ISDN call transfer failure occurs, the device sends a SIP NOTIFY message with a SIP 603 Decline response.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) The device performs a hairpin TDM transfer upon ISDN call transfer.</li> <li><b>[1]</b> = Hairpin TDM transfer is disabled.</li> </ul>
Web: Enable QSIG Transfer Update CLI: qsig-xfer-update <b>[EnableQSIGTransferUpdate]</b>	<p>Determines whether the device interworks QSIG Facility messages with CallTransferComplete or CallTransferUpdate invoke application protocol data units (APDU) to SIP UPDATE messages with P-Asserted-Identity and optional Privacy headers. This feature is supported for IP-to-Tel and Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Ignores QSIG Facility messages with CallTransferComplete or CallTransferUpdate invokes.</li> <li><b>[1]</b> Enable</li> </ul> <p>For example, assume A and C are PBX call parties and B is the SIP IP phone:</p> <ol style="list-style-type: none"> <li>1 A calls B; B answers the call.</li> <li>2 A places B on hold and calls C; C answers the call.</li> <li>3 A performs a call transfer (the transfer is done internally by the PBX); B and C are connected to one another.</li> </ol> <p>In the above example, the PBX updates B that it is now talking with C. The PBX updates this by sending a QSIG Facility message with CallTransferComplete invoke APDU. The device interworks this message to a SIP UPDATE message containing a P-Asserted-Identity header with the number and name derived from the QSIG CallTransferComplete RedirectionNumber and RedirectionName.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For IP-to-Tel calls, the RedirectionNumber and RedirectionName in the CallTransferComplete invoke is derived from the P-Asserted-Identity and Privacy headers in the received SIP INFO message.</li> <li>To include the P-Asserted-Identity header in outgoing SIP UPDATE messages, set the AssertedIDMode parameter to <b>Add P-Asserted-Identity</b>.</li> </ul>
EMS: CAS Detection Of Hook Flash CLI: is-cas-sndhook-flsh <b>[CASSendHookFlash]</b>	<p>Enables sending Wink signal toward CAS trunks.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul> <p>If the device receives a mid-call SIP INFO message with flashhook event body (as shown below) and this parameter is set to 1, the device generates a wink signal toward the CAS trunk. The CAS wink signal is done by changing the A bit from 1 to 0, and then back to 1 for 450 msec.</p> <pre> INFO sip:4505656002@192.168.13.40:5060 SIP/2.0 Via: SIP/2.0/UDP 192.168.13.2:5060 From: &lt;sip:06@192.168.13.2:5060&gt; To: &lt;sip:4505656002@192.168.13.40:5060&gt;;tag=132878796-</pre>

Parameter	Description
	1040067870294 Call-ID: 0010-0016-D69A7DA8-1@192.168.13.2 CSeq:2 INFO Content-Type: application/broadsoft Content-Length: 17 event flashhook <b>Note:</b> This parameter is applicable only to T1 CAS protocols.

### 59.11.8 Answer and Disconnect Supervision Parameters

The answer and disconnect supervision parameters are described in the table below.

#### Answer and Disconnect Parameters

Parameter	Description
Web: Answer Supervision EMS: Enable Voice Detection CLI: answer-supervision <b>[EnableVoiceDetection]</b>	<p>Enables the sending of SIP 200 OK upon detection of speech, fax, or modem.</p> <ul style="list-style-type: none"> <li><b>[1]</b> Yes = The device sends a SIP 200 OK (in response to an INVITE message) when speech, fax, or modem is detected from the Tel side.</li> <li><b>[0]</b> No = (Default) The device sends a SIP 200 OK only after it completes dialing to the Tel side.</li> </ul> <p>Typically, this feature is used only when early media (enabled using the EnableEarlyMedia parameter) is used to establish the voice path before the call is answered.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>FXO interfaces: This feature is applicable only to one-stage dialing (FXO).</li> <li>Digital interfaces: To activate this feature, set the EnableDSPMPDetectors parameter to 1.</li> <li>Digital interfaces: This feature is applicable only when the protocol type is CAS.</li> </ul>
Web/EMS: Max Call Duration (min) CLI: mx-call-duration <b>[MaxCallDuration]</b>	<p>Defines the maximum duration (in minutes) of a call. If this duration is reached, the device terminates the call. This feature is useful for ensuring available resources for new calls, by ensuring calls are properly terminated.</p> <p>The valid range is 0 to 35,791. The default is 0 (i.e., no limitation).</p>
CLI: configure voip > sip advanced-settings > set mn-call-duration <b>[MinCallDuration]</b>	<p>Defines the minimum call duration (in seconds) for the Tel side. If an established call is terminated by the IP side before this duration expires, the device terminates the call with the IP side, but delays the termination toward the Tel side until this timeout expires.</p> <p>The valid value range is 0 to 10 seconds, where 0 (default) disables this feature.</p> <p>For example: assume the minimum call duration is set to 10 seconds and an IP phone hangs up a call established with a BRI phone after 2 seconds. As the call duration is less than the minimum call duration, the device does not disconnect the call on the Tel side. However, it sends a SIP 200 OK immediately upon receipt of the BYE to disconnect from the IP phone. The call is disconnected from the Tel side only when the call duration is greater than or equal to the minimum call duration.</p> <p><b>Notes:</b></p>

Parameter	Description
	<ul style="list-style-type: none"> <li>This parameter is applicable to IP-to-Tel and Tel-to-IP calls.</li> <li>This parameter is applicable only to ISDN and CAS protocols.</li> </ul>
Web/EMS: Disconnect on Dial Tone CLI: disc-on-dial-tone <b>[DisconnectOnDialTone]</b>	<p>Determines whether the device disconnects a call when a dial tone is detected from the PBX.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Call is not released.</li> <li><b>[1]</b> Enable = Call is released if a dial tone is detected on the device's FXO port.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to FXO interfaces.</li> <li>This option is in addition to the mechanism that disconnects a call when either busy or reorder tones are detected.</li> </ul>
Web: Send Digit Pattern on Connect EMS: Connect Code CLI: digit-pttrn-on-conn <b>[TelConnectCode]</b>	<p>Defines a digit pattern to send to the Tel side after a SIP 200 OK is received from the IP side. The digit pattern is a user-defined DTMF sequence that is used to indicate an answer signal (e.g., for billing). The valid range is 1 to 8 characters.</p> <p><b>Note:</b> This parameter is applicable to FXO/CAS.</p>
Web: Disconnect on Broken Connection EMS: Disconnect Calls on Broken Connection CLI: disc-broken-conn <b>[DisconnectOnBrokenConnection]</b>	<p>Determines whether the device releases the call if RTP packets are not received within a user-defined timeout.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No</li> <li><b>[1]</b> Yes (default)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The timeout is configured by the BrokenConnectionEventTimeout parameter.</li> <li>This feature is applicable only if the RTP session is used without Silence Compression. If Silence Compression is enabled, the device doesn't detect a broken RTP connection.</li> <li>During a call, if the source IP address (from where the RTP packets are received) is changed without notifying the device, the device filters these RTP packets. To overcome this, set the DisconnectOnBrokenConnection parameter to 0; 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.</li> <li>This parameter can also be configured in an IP Profile.</li> </ul>
Web: Broken Connection Timeout EMS: Broken Connection Event Timeout CLI: broken-connection-event-timeout <b>[BrokenConnectionEventTimeout]</b>	<p>Defines the time period (in 100-msec units) after which a call is disconnected if an RTP packet is not received.</p> <p>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).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only if the parameter DisconnectOnBrokenConnection is set to 1.</li> <li>Currently, this feature functions only if Silence Suppression is disabled.</li> </ul>
Web: Disconnect Call on Silence Detection EMS: Disconnect On Detection Of Silence CLI: disc-on-silence-det <b>[EnableSilenceDisconn]</b>	<p>Determines whether calls are disconnected after detection of silence.</p> <ul style="list-style-type: none"> <li><b>[1]</b> Yes = The device disconnects calls in which silence occurs (in both call directions) for more than a user-defined time.</li> <li><b>[0]</b> No = (Default) Call is not disconnected when silence is detected.</li> </ul> <p>The silence duration can be configured by the FarEndDisconnectSilencePeriod parameter (default 120).</p>

Parameter	Description
<b>ect]</b>	<b>Note:</b> To activate this feature, set the parameters EnableSilenceCompression and FarEndDisconnectSilenceMethod to 1.
Web: Silence Detection Period <b>[sec]</b> EMS: Silence Detection Time Out <b>[FarEndDisconnectSilencePeriod]</b>	Defines the duration of the silence period (in seconds) after which the call is disconnected. The range is 10 to 28,800 (i.e., 8 hours). The default is 120 seconds. <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: Silence Detection Method <b>[FarEndDisconnectSilenceMethod]</b>	Determines the silence detection method. <ul style="list-style-type: none"> <li><b>[0]</b> None = Silence detection option is disabled.</li> <li><b>[1]</b> Packets Count = According to packet count.</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
<b>[FarEndDisconnectSilenceThreshold]</b>	Defines the threshold of the packet count (in percentages) below which is considered silence by the device. The valid range is 1 to 100%. The default is 8%. <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only if silence is detected according to packet count (FarEndDisconnectSilenceMethod is set to 1).</li> <li>For this parameter to take effect, a device reset is required.</li> </ul>
<b>[BrokenConnectionDurationSilence]</b>	Enables the generation of the BrokenConnection event during a silence period if the channel's NoOp feature is enabled (using the parameter NoOpEnable) and if the channel stops receiving NoOp RTP packets. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Web: Trunk Alarm Call Disconnect Timeout CLI: trk-alm-call-disc-to <b>[TrunkAlarmCallDisconnectTimeout]</b>	Defines the duration (in seconds) to wait after an E1/T1 trunk "Red" alarm (LOS / LOF) is raised, before the device disconnects the SIP call. If this timeout expires and the alarm is still raised, the device sends a SIP BYE message to terminate the call. If the alarm is cleared before this timeout expires, the call is not terminated, but continues as normal. The range is 1 to 3600. The default is 0 (20 for E1 and 40 for T1).
Web: Disconnect Call on Busy Tone Detection (ISDN) EMS: Isdn Disconnect On Busy Tone CLI: disc-on-bsy-tone-i <b>[ISDNDisconnectOnBusyTone]</b>	Determines whether a call is disconnected upon detection of a busy tone (for ISDN). <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Do not disconnect call upon detection of busy tone.</li> <li><b>[1]</b> Enable = Disconnect call upon detection of busy tone.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to ISDN protocols.</li> <li>IP-to-ISDN calls are disconnected on detection of SIT tones only in call alert state. If the call is in connected state, the SIT does not disconnect the calls. Detection of busy or reorder tones disconnects the IP-to-ISDN calls also in call connected state.</li> <li>For IP-to-CAS calls, detection of busy, reorder, or SIT tones disconnect the calls in any call state.</li> </ul>
Web: Disconnect Call on Busy Tone Detection EMS: Disconnect On Detection End Tones CLI: disc-on-bsy-tone-c <b>[DisconnectOnBusyTone]</b>	Determines whether a call is disconnected upon detection of a busy tone. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Call is not disconnected upon detection of a busy tone.</li> <li><b>[1]</b> Enable = (Default) Call is released upon detection of busy or reorder (fast busy) tone.</li> </ul> <b>Notes:</b>

Parameter	Description
	<ul style="list-style-type: none"> <li>Digital interfaces: This parameter is applicable only to CAS protocols.</li> <li>Analog interfaces: This parameter is applicable only to FXO interfaces.</li> <li>This parameter is also applicable to the IP-to-IP application.</li> <li>This parameter can also be configured in a Tel Profile.</li> </ul>
Polarity (Current) Reversal for Call Release (Analog Interfaces) Parameters	
<b>[SetDefaultLinePolarity State]</b> CLI: fxs-fxo > default-linepolarity-state	<p>Defines the FXO line polarity, required for DID signaling.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Positive line polarity</li> <li><b>[1]</b> = Negative line polarity</li> <li><b>[2]</b> = (Default) Auto - The device detects the polarity upon power-up or upon insertion of the RJ-11 cable, and uses it as a reference polarity.</li> </ul> <p>Typically, if the RJ-11 cabling is connected correctly (without crossing, Tip to Tip, Ring to Ring), the Tip line is positive compared to the Ring line. In this case, set this parameter to 0. With this configuration, the device assumes that the idle line polarity is Tip line positive.</p> <p>When the device receives a SIP INVITE, it checks the FXO line polarity. If the polarity is "Reversed", it skips this FXO line and goes to the next line.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To take advantage of this new feature, configure all FXO lines as a single Trunk Group with ascending or descending channel select mode, and configure routing rules to route incoming INVITE messages to this Trunk Group.</li> <li>This parameter is applicable only to FXO interfaces.</li> </ul>
Web: Enable Polarity Reversal EMS: Enable Reversal Polarity CLI: polarity-rvrsl <b>[EnableReversalPolarity]</b>	<p>Enables the polarity reversal feature for call release.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Disable the polarity reversal service.</li> <li><b>[1]</b> Enable = Enable the polarity reversal service.</li> </ul> <p>If the polarity reversal service is enabled, the FXS interface changes the line polarity on call answer and then changes it back on call release. The FXO interface sends a 200 OK response when polarity reversal signal is detected (applicable only to one-stage dialing) and releases a call when a second polarity reversal signal is detected.</p> <p><b>Note:</b> This parameter can also be configured in a Tel Profile.</p>
Web/EMS: Enable Current Disconnect CLI: current-disc <b>[EnableCurrentDisconnect]</b>	<p>Enables call release upon detection of a Current Disconnect signal.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Disable the current disconnect service.</li> <li><b>[1]</b> Enable = Enable the current disconnect service.</li> </ul> <p>If the current disconnect service is enabled:</p> <ul style="list-style-type: none"> <li>The FXO releases a call when a current disconnect signal is detected on its port.</li> <li>The FXS interface generates a 'Current Disconnect Pulse' after a call is released from IP.</li> </ul> <p>The current disconnect duration is configured by the CurrentDisconnectDuration parameter. The current disconnect threshold (FXO only) is configured by the CurrentDisconnectDefaultThreshold parameter. The frequency at which the analog line voltage is sampled is configured by the TimeToSampleAnalogLineVoltage parameter.</p>

Parameter	Description
	<b>Note:</b> This parameter can also be configured in a Tel Profile.
EMS: Polarity Reversal Type CLI: polarity-reversal-type <b>[PolarityReversalType]</b>	<p>Defines the voltage change slope during polarity reversal or wink.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Soft reverse polarity.</li> <li><b>[1]</b> = Hard reverse polarity.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to FXS interfaces.</li> <li>Some Caller ID signals use reversal polarity and/or Wink signals. In these cases, it is recommended to set the parameter PolarityReversalType to 1 (Hard).</li> <li>For this parameter to take effect, a device reset is required.</li> </ul>
EMS: Current Disconnect Duration CLI: current-disconnect-duration <b>[CurrentDisconnectDuration]</b>	<p>Defines the duration (in msec) of the current disconnect pulse. The range is 200 to 1500. The default is 900.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable for FXS and FXO interfaces.</li> <li>The FXO interface detection window is 100 msec below the parameter's value and 350 msec above the parameter's value. For example, if this parameter is set to 400 msec, then the detection window is 300 to 750 msec.</li> <li>For this parameter to take effect, a device reset is required.</li> </ul>
<b>[CurrentDisconnectDefaultThreshold]</b>	<p>Defines the line voltage threshold at which a current disconnect detection is considered.</p> <p>The valid range is 0 to 20 Volts. The default is 4 Volts.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to FXO interfaces.</li> <li>For this parameter to take effect, a device reset is required.</li> </ul>
CLI: time-to-sample-analog-line-voltage <b>[TimeToSampleAnalogLineVoltage]</b>	<p>Defines the frequency at which the analog line voltage is sampled (after offhook), for detection of the current disconnect threshold.</p> <p>The valid range is 100 to 2500 msec. The default is 1000 msec.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to FXO interfaces.</li> <li>For this parameter to take effect, a device reset is required.</li> </ul>

## 59.11.9 Tone Parameters

This subsection describes the device's tone parameters.

### 59.11.9.1 Telephony Tone Parameters

The telephony tone parameters are described in the table below.

**Tone Parameters**

Parameter	Description
CLI: help-tone-4-ip2ip <b>[PlayHeldToneForIP2IP]</b>	<p>Enables playing a held tone to an IP-to-IP leg instead of placing it on hold.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disabled. The device interworks the re-INVITE with 'a=inactive' from one SIP leg to another SIP leg.</li> <li><b>[1]</b> = Enabled. The device plays a held tone to the IP if it</li> </ul>



Parameter	Description
	<p>receives a re-INVITE with 'a=inactive' in the SDP from the party initiating the call hold. The held tone must be configured in the CPT file.</p> <p><b>Note:</b> This parameter is applicable only to the IP-to-IP application.</p>
Web: SIP Hold Behavior CLI: sip-hold-behavior <b>[SIPHoldBehavior]</b>	<p>Enables the device to handle incoming re-INVITE messages with the "a=sendonly" attribute in the SDP, in the same way as if an "a=inactive" is received in the SDP. When enabled, the device plays a held tone to the Tel phone and responds with a SIP 200 OK containing the "a=recvonly" attribute in the SDP.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Web/EMS: Dial Tone Duration <b>[sec]</b> CLI: dt-duration <b>[TimeForDialTone]</b>	<p>Defines the duration (in seconds) that the dial tone is played (for digital interfaces, to an ISDN terminal).</p> <p>For digital interfaces: This parameter is applicable for overlap dialing when ISDNInCallsBehavior is set to 65536. The dial tone is played if the ISDN Setup message doesn't include the called number.</p> <p>The valid range is 0 to 60. The default is 5.</p> <p>For analog interfaces: FXS interfaces play the dial tone after the phone is picked up (off-hook). FXO interfaces play the dial tone after the port is seized in response to ringing (from PBX/PSTN). The valid range is 0 to 60. The default time is 16.</p> <p>Notes for analog interfaces:</p> <ul style="list-style-type: none"> <li>▪ During play of dial tone, the device waits for DTMF digits.</li> <li>▪ This parameter is not applicable when Automatic Dialing is enabled.</li> </ul>
Web/EMS: Stutter Tone Duration CLI: sttr-tone-duration <b>[StutterToneDuration]</b>	<p>Defines the duration (in msec) of the confirmation tone. A stutter tone is played (instead of a regular dial tone) when a Message Waiting Indication (MWI) is received. The stutter tone is composed of a confirmation tone (Tone Type #8), which is played for the defined duration (StutterToneDuration) followed by a stutter dial tone (Tone Type #15). Both these tones are defined in the CPT file.</p> <p>The range is 1,000 to 60,000. The default is 2,000 (i.e., 2 seconds).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to FXS interfaces.</li> <li>▪ If you want to configure the duration of the confirmation tone to longer than 16 seconds, you must increase the value of the parameter TimeForDialTone accordingly.</li> <li>▪ The MWI tone takes precedence over the call forwarding reminder tone. For more information on MWI, see Message Waiting Indication on page 358.</li> </ul>
Web: FXO AutoDial Play BusyTone EMS: Auto Dial Play Busy Tone CLI: fxo-autodial-play-bsytn <b>[FXOAutoDialPlayBusyTone]</b>	<p>Determines whether the device plays a busy / reorder tone to the PSTN side if a Tel-to-IP call is rejected by a SIP error response (4xx, 5xx or 6xx). If a SIP error response is received, the device seizes the line (off-hook), and then plays a busy / reorder tone to the PSTN side (for the duration defined by the parameter TimeForReorderTone). After playing the tone, the line is released (on-hook).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[1]</b> = Enable</li> </ul> <p><b>Note:</b> This parameter is applicable only to FXO interfaces.</p>
Web: Hotline Dial Tone Duration EMS: Hot Line Tone Duration CLI: hotline-dt-dur <b>[HotLineToneDuration]</b>	<p>Defines the duration (in seconds) of the hotline dial tone. If no digits are received during this duration, the device initiates a call to a user-defined number (configured in the Automatic Dialing table - TargetOfChannel - see Configuring Automatic Dialing on page 396).</p> <p>The valid range is 0 to 60. The default is 16.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable to FXS and FXO interfaces.</li> <li>▪ You can define the Hotline duration per FXS/FXO port using the Automatic Dialing table.</li> </ul>
Web/EMS: Reorder Tone Duration <b>[sec]</b> CLI: reorder-tone-duration <b>[TimeForReorderTone]</b>	<p>For analog interfaces: Defines the duration (in seconds) that the device plays a busy or reorder tone before releasing the line. Typically, after playing the busy or reorder tone for this duration, the device starts playing an offhook warning tone.</p> <p>For digital interfaces: Defines the duration (in seconds) that the CAS device plays a busy or reorder tone before releasing the line. The valid range is 0 to 254. The default is 0 seconds for analog interfaces and 10 seconds for digital interfaces. Note that the Web interface denotes the default value (for analog and digital interfaces) as a string value of "255".</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The selected busy or reorder tone is according to the SIP release cause code received from IP.</li> <li>▪ This parameter is also applicable for ISDN when the PlayBusyTone2ISDN parameter is set to 2.</li> <li>▪ This parameter can also be configured in a Tel Profile.</li> </ul>
Web: Time Before Reorder Tone <b>[sec]</b> EMS: Time For Reorder Tone CLI: time-b4-reordr-tn <b>[TimeBeforeReorderTone]</b>	<p>Defines the delay interval (in seconds) from when the device receives a SIP BYE message (i.e., remote party terminates call) until the device starts playing a reorder tone to the FXS phone.</p> <p>The valid range is 0 to 60. The default is 0.</p> <p><b>Note:</b> This parameter is applicable only to FXS interfaces.</p>
Web: Cut Through Reorder Tone Duration <b>[sec]</b> CLI: cut-thru-reord-dur <b>[CutThroughTimeForReOrderTone]</b>	<p>Defines the duration (in seconds) of the reorder tone played to the PSTN side after the IP call party releases the call, for the Cut-Through feature. After the tone stops playing, an incoming call is immediately answered if the FXS is off-hooked (for analog interfaces) or the PSTN is connected (for digital interfaces).</p> <p>The valid values are 0 to 30. The default is 0 (i.e., no reorder tone is played).</p> <p><b>Note:</b> To enable the Cut-Through feature, use the DigitalCutThrough (for CAS channels) or CutThrough (for FXS channels) parameters.</p>
Web/EMS: Enable Comfort Tone CLI: comfort-tone <b>[EnableComfortTone]</b>	<p>Determines whether the device plays a comfort tone (Tone Type #18) to the FXS/FXO endpoint after a SIP INVITE is sent and before a SIP 18x response is received.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> This parameter is applicable to FXS and FXO interfaces.</p>



Parameter	Description
<b>[WarningToneDuration]</b>	<p>Defines the duration (in seconds) for which the offhook warning tone is played to the user.</p> <p>The valid range is -1 to 2,147,483,647. The default is 600.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>A negative value indicates that the tone is played infinitely.</li> <li>This parameter is applicable only to analog interfaces.</li> </ul>
Web: Play Busy Tone to Tel CLI: play-busy-tone-2tel <b>[PlayBusyTone2ISDN]</b>	<p>Enables the device to play a busy or reorder tone to the PSTN after a Tel-to-IP call is released.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Don't Play = (Default) Immediately sends an ISDN Disconnect message.</li> <li><b>[1]</b> Play when Disconnecting = Sends an ISDN Disconnect message with PI = 8 and plays a busy or reorder tone to the PSTN (depending on the release cause).</li> <li><b>[2]</b> Play before Disconnect = Delays the sending of an ISDN Disconnect message for a user-defined time (configured by the TimeForReorderTone parameter) and plays a busy or reorder tone to the PSTN. This is applicable only if the call is released from the IP <b>[Busy Here (486) or Not Found (404)]</b> before it reaches the Connect state; otherwise, the Disconnect message is sent immediately and no tones are played.</li> </ul> <p><b>Note:</b> This parameter is applicable only to digital PSTN interfaces.</p>
Web: Play Ringback Tone to Tel EMS: Play Ring Back Tone To Tel CLI: play-rbt2tel <b>[PlayRBTone2Tel]</b>	<p>Determines the playing method of the ringback tone to the Tel (for analog interfaces) or Trunk (for digital interfaces) side. For digital interfaces: This parameter applies to all trunks that are not configured by the PlayRBTone2Trunk parameter (which defines ringback tone per Trunk).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Don't Play =               <ul style="list-style-type: none"> <li>✓ Analog Interfaces: Ringback tone is not played.</li> <li>✓ Digital Interfaces: The device configured for ISDN / CAS doesn't play a ringback tone. No PI is sent to the ISDN unless the ProgressIndicator2ISDN_x parameter is configured differently.</li> </ul> </li> <li><b>[1]</b> Play on Local =               <ul style="list-style-type: none"> <li>✓ Analog Interfaces: Plays a ringback tone to the Tel side of the call when a SIP 180/183 response is received.</li> <li>✓ Digital Interfaces: The device configured for CAS plays a local ringback tone to the PSTN upon receipt of a SIP 180 Ringing response (with or without SDP). Note that the receipt of a 183 response does not cause the device configured for CAS to play a ringback tone (unless the SIP183Behaviour parameter is set to 1). The device configured for ISDN operates according to the LocalISDNRBSources parameter:                   <ol style="list-style-type: none"> <li>If the device receives a 180 Ringing response (with or without SDP) and the LocalISDNRBSources parameter is set to 1, it plays a ringback tone and sends an ISDN Alert with PI = 8 (unless the ProgressIndicator2ISDN_x parameter is configured differently).</li> <li>If the LocalISDNRBSources parameter is set to 0, the device doesn't play a ringback tone and an Alert message without PI is sent to the ISDN. In this case, the PBX /</li> </ol> </li> </ul> </li> </ul>

Parameter	Description
	<p>PSTN plays the ringback tone to the originating terminal. Note that the receipt of a 183 response does not cause the device configured for ISDN to play a ringback tone; the device issues a Progress message (unless SIP183Behaviour is set to 1). If the SIP183Behaviour parameter is set to 1, the 183 response is handled the same way as a 180 Ringing response.</p> <ul style="list-style-type: none"> <li>▪ <b>[2] Prefer IP = (Default):</b> <ul style="list-style-type: none"> <li>✓ Analog Interfaces: Plays a ringback tone to the Tel side only if a 180/183 response without SDP is received. If 180/183 with SDP message is received, the device cuts through the voice channel and doesn't play the ringback tone.</li> <li>✓ Digital Interfaces: Plays according to 'Early Media'. If a SIP 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the device configured for ISDN / CAS doesn't play the ringback tone; PI = 8 is sent in an ISDN Alert message (unless the ProgressIndicator2ISDN_x parameter is configured differently). If a 180 response is received, but the 'early media' voice channel is not opened, the device configured for CAS plays a ringback tone to the PSTN. The device configured for ISDN operates according to the LocalISDNRBSource parameter: <ul style="list-style-type: none"> <li>1) If LocalISDNRBSource is set to 1, the device plays a ringback tone and sends an ISDN Alert with PI = 8 to the ISDN (unless the ProgressIndicator2ISDN_x parameter is configured differently).</li> <li>2) If LocalISDNRBSource is set to 0, the device doesn't play a ringback tone. No PI is sent in the ISDN Alert message (unless the ProgressIndicator2ISDN_x parameter is configured differently). In this case, the PBX / PSTN plays a ringback tone to the originating terminal.</li> </ul> </li> </ul> </li> <li>▪ <b>[3] Play Local Until Remote Media Arrive =</b> Plays a ringback tone according to received media. The behaviour is similar to <b>[2]</b>. If a SIP 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the device plays a local ringback tone if there are no prior received RTP packets. The device stops playing the local ringback tone as soon as it starts receiving RTP packets. At this stage, if the device receives additional 18x responses, it does not resume playing the local ringback tone. Note that for ISDN trunks, this option is applicable only if the LocalISDNRBSource parameter is set to 1.</li> </ul> <p><b>Note:</b> This parameter is applicable to the Gateway and IP-to-IP applications.</p>
Web: Play Ringback Tone to Trunk CLI: play-rbt-to-trk	Determines the playing method of the ringback tone to the trunk side, per trunk. <ul style="list-style-type: none"> <li>▪ <b>[-1] Not configured = (Default)</b> The settings of the</li> </ul>

Parameter	Description
[PlayRBTone2Trunk_x]	<p>PlayRBTone2Tel parameter is used.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Don't Play = When the device is configured for ISDN / CAS, it doesn't play a ringback tone. No Progress Indicator (PI) is sent to the ISDN unless the ProgressIndicator2ISDN_x parameter is configured differently.</li> <li>▪ <b>[1]</b> Play on Local = When the device is configured for CAS, it plays a local ringback tone to the PSTN upon receipt of a SIP 180 Ringing response (with or without SDP). Note that the receipt of a SIP 183 response does not cause the device configured for CAS to play a ringback tone (unless the SIP183Behaviour parameter is set to 1).</li> </ul> <p>When the device is configured for ISDN, it operates according to the LocalISDNRBSource parameter, as follows:</p> <ul style="list-style-type: none"> <li>✓ If the device receives a SIP 180 Ringing response (with or without SDP) and the LocalISDNRBSource parameter is set to 1, it plays a ringback tone and sends an ISDN Alert with PI = 8 (unless the ProgressIndicator2ISDN_x parameter is configured differently).</li> <li>✓ If the LocalISDNRBSource parameter is set to 0, the device doesn't play a ringback tone and an Alert message without PI is sent to the ISDN. In this case, the PBX / PSTN plays the ringback tone to the originating terminal. Note that the receipt of a 183 response does not cause the device to play a ringback tone; the device sends a Progress message (unless SIP183Behaviour is set to 1). If the SIP183Behaviour parameter is set to 1, the 183 response is handled the same way as a 180 Ringing response.</li> <li>▪ <b>[2]</b> Prefer IP = Plays according to 'Early Media'. If a SIP 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the device configured for ISDN / CAS doesn't play the ringback tone; PI = 8 is sent in an ISDN Alert message (unless the ProgressIndicator2ISDN_x parameter is configured differently). If a 180 response is received, but the 'early media' voice channel is not opened, the device configured for CAS plays a ringback tone to the PSTN. The device configured for ISDN operates according to the LocalISDNRBSource parameter: <ul style="list-style-type: none"> <li>✓ If LocalISDNRBSource is set to 1, the device plays a ringback tone and sends an ISDN Alert with PI = 8 to the ISDN (unless the ProgressIndicator2ISDN_x parameter is configured differently).</li> <li>✓ If LocalISDNRBSource is set to 0, the device doesn't play a ringback tone. No PI is sent in the ISDN Alert message (unless the ProgressIndicator2ISDN_x parameter is configured differently). In this case, the PBX / PSTN plays a ringback tone to the originating terminal. Note that the receipt of a 183 response results in an ISDN Progress message (unless SIP183Behaviour is set to 1). If SIP183Behaviour is set to 1 (183 is handled the same way as a 180 with SDP), the device sends an Alert message with PI = 8 without playing a ringback tone.</li> </ul> </li> <li>▪ <b>[3]</b> Play Local Until Remote Media Arrive = Plays tone according to received media. The behaviour is similar to option</li> </ul>

Parameter	Description
	<p><b>[2].</b> If a SIP 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the device plays a local ringback tone if there are no prior received RTP packets. The device stops playing the local ringback tone as soon as it starts receiving RTP packets. At this stage, if the device receives additional 18x responses, it does not resume playing the local ringback tone. Note that for ISDN trunks, this option is applicable only if LocalISDNRBSrc is set to 1.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only to the Gateway (GW) application (i.e., not the IP-to-IP application).</li> <li>▪ This parameter is applicable only to digital PSTN interfaces.</li> <li>▪ The x in the ini file parameter denotes the trunk number, where 0 is Trunk 1.</li> </ul>
Web: Play Ringback Tone to IP EMS: Play Ring Back Tone To IP CLI: play-rbt-2ip <b>[PlayRBTone2IP]</b>	<p>Determines whether the device plays a ringback tone to the IP side for IP-to-Tel calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Don't Play = (Default) Ringback tone isn't played.</li> <li>▪ <b>[1]</b> Play = Ringback tone is played after SIP 183 session progress response is sent.</li> </ul> <p>For digital modules: If configured to 1 ('Play') and EnableEarlyMedia is set to 1, the device plays a ringback tone according to the following:</p> <ul style="list-style-type: none"> <li>▪ For CAS interfaces: the device opens a voice channel, sends a 183+SDP response, and then plays a ringback tone to IP.</li> <li>▪ For ISDN interfaces: if a Progress or an Alerting message with PI (1 or 8) is received from the ISDN, the device opens a voice channel, sends a 183+SDP or 180+SDP response, but doesn't play a ringback tone to IP. If PI (1 or 8) is received from the ISDN, the device assumes that ringback tone is played by the ISDN switch. Otherwise, the device plays a ringback tone to IP after receiving an Alerting message from the ISDN. It sends a 180+SDP response, signaling to the calling party to open a voice channel to hear the played ringback tone.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To enable the device to send a 183/180+SDP responses, set the EnableEarlyMedia parameter to 1.</li> <li>▪ If the EnableDigitDelivery parameter is set to 1, the device doesn't play a ringback tone to IP and doesn't send 183 or 180+SDP responses.</li> <li>▪ This parameter can also be configured in an IP Profile.</li> </ul>
Web: Play Local RBT on ISDN Transfer EMS: Play RBT On ISDN Transfer CLI: play-l-rbt-isdn-trsfr <b>[PlayRBTOnISDNTransfer]</b>	<p>Determines whether the device plays a local ringback tone for ISDN's Two B Channel Transfer (TBCT), Release Line Trunk (RLT), or Explicit Call Transfer (ECT) call transfers to the originator when the second leg receives an ISDN Alerting or Progress message.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Don't Play (default)</li> <li>▪ <b>[1]</b> Play</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For Blind transfer, the local ringback tone is played to first call PSTN party when the second leg receives the ISDN Alerting or Progress message.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>For Consulted transfer, the local ringback tone is played when the second leg receives ISDN Alerting or Progress message if the Progress message is received after a SIP REFER.</li> <li>This parameter is applicable only if the parameter SendISDNTransferOnConnect is set to 1.</li> </ul>
Web: MFC R2 Category EMS: R2 Category CLI: mfc2-category <b>[R2Category]</b>	Defines the tone for MFC R2 calling party category (CPC). The parameter provides information on the calling party such as National or International call, Operator or Subscriber and Subscriber priority.  The value range is 1 to 15 (defining one of the MFC R2 tones). The default is 1.
Tone Index Table	
Web: Tone Index Table EMS: Analog Gateway Provisioning > Tone Index CLI: configure voip > gw analoggw tone-index <b>[ToneIndex]</b>	This table parameter configures the Tone Index table, which allows you to define distinctive ringing and call waiting tones per FXS endpoint (or for a range of FXS endpoints).  The format of this parameter is as follows: <b>[ToneIndex]</b> FORMAT ToneIndex_Index = ToneIndex_FXSPort_First, ToneIndex_FXSPort_Last, ToneIndex_SourcePrefix, ToneIndex_DestinationPrefix, ToneIndex_PriorityIndex; <b>[ToneIndex]</b>  For example, the configuration below plays the tone Index #3 to FXS ports 1 and 2 if the source number prefix of the received call is 20. ToneIndex 1 = 1, 2, 20*, , 3;  <b>Note:</b> For a detailed description of this table, see Configuring FXS Distinctive Ringing and Call Waiting Tones per Source/Destination Number.

### 59.11.9.2 Tone Detection Parameters

The signal tone detection parameters are described in the table below.

**Tone Detection Parameters**

Parameter	Description
EMS: DTMF Enable CLI: DTMF-detector-enable <b>[DTMFDetectorEnable]</b>	Enables the detection of DTMF signaling. <ul style="list-style-type: none"> <li><b>[0]</b> = Disable</li> <li><b>[1]</b> = Enable (default)</li> </ul>
EMS: MF R1 Enable CLI: MFR1-detector-enable <b>[MFR1DetectorEnable]</b>	Enables the detection of MF-R1 signaling. <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul>
EMS: R1.5 Detection Standard <b>[R1DetectionStandard]</b>	Determines the MF-R1 protocol used for detection. <ul style="list-style-type: none"> <li><b>[0]</b> = ITU (default)</li> <li><b>[1]</b> = R1.5</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
EMS: User Defined Tone Enable CLI: user-defined-tones-	Enables the detection of User Defined Tones signaling, applicable for Special Information Tone (SIT) detection.

Parameter	Description
detector-enable [UserDefinedToneDetectorEnable]	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul>
EMS: SIT Enable CLI: SIT-detector-enable [SITDetectorEnable]	<p>Enables SIT detection according to the ITU-T recommendation E.180/Q.35.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul> <p>To disconnect IP-to-ISDN calls when a SIT tone is detected, the following parameters must be configured:</p> <ul style="list-style-type: none"> <li>▪ SITDetectorEnable = 1</li> <li>▪ UserDefinedToneDetectorEnable = 1</li> <li>▪ ISDNDisconnectOnBusyTone = 1 (applicable for Busy, Reorder and SIT tones)</li> </ul> <p>Another parameter for handling the SIT tone is SITQ850Cause, which determines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when a SIT tone is detected on an IP-to-Tel call.</p> <p>To disconnect IP-to-CAS calls when a SIT tone is detected, the following parameters must be configured (applicable to FXO interfaces):</p> <ul style="list-style-type: none"> <li>▪ SITDetectorEnable = 1</li> <li>▪ UserDefinedToneDetectorEnable = 1</li> <li>▪ DisconnectOnBusyTone = 1 (applicable for busy, reorder, and SIT tones)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ The IP-to-ISDN call is disconnected on detection of a SIT tone only in call alert state. If the call is in connected state, the SIT does not disconnect the call. Detection of busy or reorder tones disconnect these calls also in call connected state.</li> <li>▪ For IP-to-CAS calls, detection of busy, reorder, or SIT tones disconnect the call in any call state.</li> </ul>
EMS: UDT Detector Frequency Deviation CLI: UDT-detector-frequency-deviation [UDTDetectorFrequencyDeviation]	<p>Defines the deviation (in Hz) allowed for the detection of each signal frequency.</p> <p>The valid range is 1 to 50. The default is 50.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: CPT Detector Frequency Deviation CLI: CPT-detector-frequency-deviation [CPTDetectorFrequencyDeviation]	<p>Defines the deviation (in Hz) allowed for the detection of each CPT signal frequency.</p> <p>The valid range is 1 to 30. The default is 10.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>



### 59.11.9.3 Metering Tone Parameters

The metering tone parameters are described in the table below.

**Metering Tone Parameters**

Parameter	Description
Web: Generate Metering Tones EMS: Metering Mode CLI: gen-mtr-tones <b>[PayPhoneMeteringMode]</b>	Determines the method used to configure the metering tones that are generated to the Tel side. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Metering tones aren't generated.</li> <li><b>[1]</b> Internal Table = Metering tones are generated according to the device's Charge Code table (using the ChargeCode parameter).</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>This parameter is applicable only to FXS interfaces and ISDN Euro trunks for sending AOC Facility messages (see Advice of Charge Services for Euro ISDN on page 388).</li> <li>If you select 'Internal Table', you must configure the Charge Codes table, using the ChargeCode parameter (see Configuring Charge Codes Table on page 393).</li> </ul>
Web: Analog Metering Type EMS: Metering Type CLI: metering-type <b>[MeteringType]</b>	Determines the metering method for generating pulses (sinusoidal metering burst frequency) by the FXS port. <ul style="list-style-type: none"> <li><b>[0]</b> 12 KHz = (Default) 12 kHz sinusoidal bursts.</li> <li><b>[1]</b> 16 KHz = 16 kHz sinusoidal bursts.</li> <li><b>[2]</b> = Polarity Reversal pulses.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>This parameter is applicable only to FXS interfaces.</li> </ul>
Web: Analog TTX Voltage Level EMS: TTX Voltage Level <b>[AnalogTTXVoltageLevel]</b>	Determines the metering signal/pulse voltage level (TTX). <ul style="list-style-type: none"> <li><b>[0]</b> 0V = 0 Vrms sinusoidal bursts.</li> <li><b>[1]</b> 0.5V = (Default) 0.5 Vrms sinusoidal bursts.</li> <li><b>[2]</b> 1V = 1 Vrms sinusoidal bursts</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>This parameter is applicable only to FXS interfaces.</li> </ul>
<b>Charge Codes Table</b>	
Web: Charge Codes Table EMS: Charge Codes CLI: configure voip > gw analoggw ChargeCode <b>[ChargeCode]</b>	This table parameter configures metering tones and their time intervals that the device's FXS interface generates to the Tel side or the E1 trunk (EuroISDN) sends in AOC Facility messages to the PSTN (i.e., PBX). The format of this parameter is as follows: <b>[ChargeCode]</b> FORMAT ChargeCode_Index = ChargeCode_EndTime1, ChargeCode_PulseInterval1, ChargeCode_PulsesOnAnswer1, ChargeCode_EndTime2, ChargeCode_PulseInterval2, ChargeCode_PulsesOnAnswer2, ChargeCode_EndTime3, ChargeCode_PulseInterval3, ChargeCode_PulsesOnAnswer3, ChargeCode_EndTime4, ChargeCode_PulseInterval4, ChargeCode_PulsesOnAnswer4; <b>[ChargeCode]</b> Where, <ul style="list-style-type: none"> <li>EndTime = Period (1 - 4) end time.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>PulseInterval = Period (1 - 4) pulse interval.</li> <li>PulsesOnAnswer = Period (1 - 4) pulses on answer.</li> </ul> <p>For example:  ChargeCode 1 = 7,30,1,14,20,2,20,15,1,0,60,1;  ChargeCode 2 = 5,60,1,14,20,1,0,60,1;  ChargeCode 3 = 0,60,1;  ChargeCode 0 = 6, 3, 1, 12, 2, 1, 18, 5, 2, 0, 2, 1;</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To associate a configured Charge Code to an outgoing Tel-to-IP call, use the Outbound IP Routing Table.</li> <li>To configure the Charge Codes table using the Web interface, see Configuring Charge Codes Table on page 393.</li> </ul>

## 59.11.10 Telephone Keypad Sequence Parameters

The telephony keypad sequence parameters are described in the table below.

**Telephone Keypad Sequence Parameters**

Parameter	Description
Web/EMS: Call Pickup Key CLI: sip-definition advanced- settings > call-pickup-key <b>[KeyCallPickup]</b>	<p>Defines the keying sequence for performing a call pick-up. Call pick-up allows the FXS endpoint to answer another telephone's incoming call by pressing this user-defined sequence of digits. When the user dials these digits (e.g., #77), the incoming call from another phone is forwarded to the user's phone.</p> <p>The valid value is a string of up to 15 characters (0-9, #, and *). The default is undefined.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Call pick-up is configured only for FXS endpoints pertaining to the same Trunk Group.</li> <li>This parameter is applicable only to FXS interfaces.</li> </ul>
<b>Prefix for External Line</b>	
<b>[Prefix2ExtLine]</b>	<p>Defines a string prefix (e.g., '9' dialed for an external line) that when dialed, the device plays a secondary dial tone (i.e., stutter tone) to the FXS line and then starts collecting the subsequently dialed digits from the FXS line.</p> <p>The valid range is a one-character string. The default is an empty string.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>You can enable the device to add this string as the prefix to the collected (and sent) digits, using the parameter AddPrefix2ExtLine.</li> <li>This parameter is applicable only to FXS interfaces.</li> </ul>
CLI: prefix-2-ext-line <b>[AddPrefix2ExtLine]</b>	<p>Determines whether the prefix string for accessing an external line (defined by the parameter Prefix2ExtLine) is added to the dialed number as the prefix and together sent to the IP destination (Tel-to-IP calls).</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul> <p>For example, if this parameter is enabled and the prefix string for</p>



Parameter	Description
	<p>the external line is defined as "9" (using the parameter Prefix2ExtLine) and the FXS user wants to make a call to destination "123", the device collects and sends all the dialed digits, including the prefix string, as "9123" to the IP destination number.</p> <p><b>Note:</b> This parameter is applicable only to FXS interfaces.</p>
<b>Hook Flash Parameters</b>	
Web: Flash Keys Sequence Style CLI: flash-key-seq-style <b>[FlashKeysSequenceStyle]</b>	<p>Determines the hook-flash key sequence for FXS interfaces.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Flash hook = (Default) Only the phone's flash button is used, according to the following scenarios:               <ul style="list-style-type: none"> <li>✓ During an existing call, if the user presses the flash button, the call is put on hold; a dial tone is heard and the user is able to initiate a second call. Once the second call is established, on-hooking transfers the first (held) call to the second call.</li> <li>✓ During an existing call, if a call comes in (call waiting), pressing the flash button places the active call on hold and answers the waiting call; pressing flash again toggles between these two calls.</li> </ul> </li> <li>▪ <b>[1]</b> Sequence 1 = Sequence of flash and digit:               <ul style="list-style-type: none"> <li>✓ Flash + 1: holds a call or toggles between two existing calls</li> <li>✓ Flash + 2: makes a call transfer.</li> <li>✓ Flash + 3: makes a three-way conference call (if the Three-Way Conference feature is enabled, i.e., the parameter Enable3WayConference is set to 1 and the parameter 3WayConferenceMode is set to 2).</li> </ul> </li> <li>▪ <b>[2]</b> Sequence 2 = Sequence of flash and digit:               <ul style="list-style-type: none"> <li>✓ Flash only: Places a call on hold.</li> <li>✓ Flash + 1:                   <ol style="list-style-type: none"> <li>1) When the device handles two calls (an active and a held call) and this key sequence is dialed, it sends a SIP BYE message to the active call and the previously held call becomes the active call.</li> <li>2) When there is an active call and an incoming waiting call, if this key sequence is dialed, the device disconnects the active call and the waiting call becomes an active call.</li> </ol> </li> <li>✓ Flash + 2: Places a call on hold and answers a call-waiting call, or toggles between active and on-hold calls.</li> <li>✓ Flash + 3: Makes a three-way conference call. This is applicable only if the Enable3WayConference parameter is set to 1 and the 3WayConferenceMode parameter is set to 2. Note that the settings of the ConferenceCode parameter is ignored.</li> <li>✓ Flash + 4: Makes a call transfer.</li> </ul> </li> </ul> <p><b>Note:</b> This parameter is applicable only to FXS interfaces.</p>
Web: Flash Keys Sequence Timeout CLI: flash-key-seq-tmout <b>[FlashKeysSequenceTimeout]</b>	<p>Defines the Flash keys sequence timeout - the time (in msec) that the device waits for digits after the user presses the Flash button (Flash Hook + Digit mode - when the parameter FlashKeysSequenceStyle is set to 1 or 2).</p> <p>The valid range is 100 to 5,000. The default is 2,000.</p>
<b>Keypad Feature - Call Forward Parameters</b>	

Parameter	Description
Web: Forward Unconditional EMS: Call Forward Unconditional CLI: fwd-unconditional <b>[KeyCFUnCond]</b>	Defines the keypad sequence to activate the immediate call forward option.
Web: Forward No Answer EMS: Call Forward No Answer CLI: fwd-no-answer <b>[KeyCFNoAnswer]</b>	Defines the keypad sequence to activate the forward on no answer option.
Web: Forward On Busy EMS: Call Forward Busy CLI: fwd-on-busy <b>[KeyCFBusy]</b>	Defines the keypad sequence to activate the forward on busy option.
Web: Forward On Busy or No Answer EMS: CF Busy Or No Answer CLI: fwd-busy-or-no-ans <b>[KeyCFBusyOrNoAnswer]</b>	Defines the keypad sequence to activate the forward on 'busy or no answer' option.
Web: Do Not Disturb EMS: CF Do Not Disturb CLI: fwd-dnd <b>[KeyCFDoNotDisturb]</b>	Defines the keypad sequence to activate the Do Not Disturb option (immediately reject incoming calls).
<p>To activate the required forward method from the telephone:</p> <ol style="list-style-type: none"> <li>4 Dial the user-defined sequence number on the keypad; a dial tone is heard.</li> <li>5 Dial the telephone number to which the call is forwarded (terminate the number with #); a confirmation tone is heard.</li> </ol>	
Web: Forward Deactivate EMS: Call Forward Deactivation CLI: fwd-deactivate <b>[KeyCFDeact]</b>	Defines the keypad sequence to deactivate any of the call forward options. After the sequence is pressed, a confirmation tone is heard.
<b>Keypad Feature - Caller ID Restriction Parameters</b>	
Web: Restricted Caller ID Activate EMS: CLIR CLI: id-restriction-act <b>[KeyCLIR]</b>	Defines the keypad sequence to activate the restricted Caller ID option. After the sequence is pressed, a confirmation tone is heard.
Web: Restricted Caller ID Deactivate EMS: CLIR Deactivation CLI: id-restriction-deact <b>[KeyCLIRDeact]</b>	Defines the keypad sequence to deactivate the restricted Caller ID option. After the sequence is pressed, a confirmation tone is heard.
<b>Keypad Feature - Hotline Parameters</b>	
Web: Hot-line Activate EMS: Hot Line CLI: hotline-act <b>[KeyHotLine]</b>	<p>Defines the keypad sequence to activate the delayed hotline option.</p> <p>To activate the delayed hotline option from the telephone, perform the following:</p> <ol style="list-style-type: none"> <li>6 Dial the user-defined sequence number on the keypad; a dial tone is heard.</li> <li>7 Dial the telephone number to which the phone automatically dials after a configurable delay (terminate the number with #);</li> </ol>

Parameter	Description
	a confirmation tone is heard.
Web: Hot-line Deactivate EMS: Hot Line Deactivation CLI: hotline-deact <b>[KeyHotLineDeact]</b>	Defines the keypad sequence to deactivate the delayed hotline option. After the sequence is pressed, a confirmation tone is heard.
<b>Keypad Feature - Transfer Parameters</b>	
<b>Note:</b> See the description of the KeyBlindTransfer parameter for this feature.	
<b>Keypad Feature - Call Waiting Parameters</b>	
Web: Call Waiting Activate EMS: Keypad Features CW CLI: cw-act <b>[KeyCallWaiting]</b>	Defines the keypad sequence to activate the Call Waiting option. After the sequence is pressed, a confirmation tone is heard.
Web: Call Waiting Deactivate EMS: Keypad Features CW Deact CLI: cw-deact <b>[KeyCallWaitingDeact]</b>	Defines the keypad sequence to deactivate the Call Waiting option. After the sequence is pressed, a confirmation tone is heard.
<b>Keypad Feature - Reject Anonymous Call Parameters</b>	
Web: Reject Anonymous Call Activate EMS: Reject Anonymous Call <b>[KeyRejectAnonymousCall]</b>	Defines the keypad sequence to activate the reject anonymous call option, whereby the device rejects incoming anonymous calls. After the sequence is pressed, a confirmation tone is heard.
Web: Reject Anonymous Call Deactivate EMS: Reject Anonymous Call Deact <b>[KeyRejectAnonymousCallDeact]</b>	Defines the keypad sequence that de-activates the reject anonymous call option. After the sequence is pressed, a confirmation tone is heard.

### 59.11.11 General FXO Parameters

The general FXO and FXS parameters are described in the table below.

**General FXO and FXS Parameters**

Parameter	Description
<b>FXS Parameters</b>	
Web: FXS Coefficient Type EMS: Country Coefficients CLI: fxs-country-coefficients <b>[FXSCountryCoefficients]</b>	<p>Determines the FXS line characteristics (AC and DC) according to USA or Europe (TBR21) standards.</p> <ul style="list-style-type: none"> <li><b>[66]</b> Europe = TBR21</li> <li><b>[70]</b> USA = (Default) United States</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>FXO Parameters</b>	
Web: FXO Coefficient Type EMS: Country Coefficients CLI: fxo-country-coefficients	Determines the FXO line characteristics (AC and DC) according to USA or TBR21 standard.

Parameter	Description
[CountryCoefficients]	<ul style="list-style-type: none"> <li>[66] Europe = TBR21</li> <li>[70] USA = (Default) United States</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
CLI: fxo-dc-termination [FXODCTermination]	<p>Defines the FXO line DC termination (i.e., resistance).</p> <ul style="list-style-type: none"> <li>[0] = (Default) DC termination is set to 50 Ohms.</li> <li>[1] = DC termination set to 800 Ohms. The termination changes from 50 to 800 Ohms only when moving from onhook to offhook.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
CLI: enable-fxo-current-limit [EnableFXOCurrentLimit]	<p>Enables limiting the FXO loop current to a maximum of 60 mA (according to the TBR21 standard).</p> <ul style="list-style-type: none"> <li>[0] = (Default) FXO line current limit is disabled.</li> <li>[1] = FXO loop current is limited to a maximum of 60 mA.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
[FXONumberOfRings]	<p>Defines the number of rings before the device's FXO interface answers a call by seizing the line.</p> <p>The valid range is 0 to 10. The default is 0.</p> <p>When set to 0, the FXO seizes the line after one ring. When set to 1, the FXO seizes the line after two rings.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only if automatic dialing is not used.</li> <li>If caller ID is enabled and if the number of rings defined by the parameter RingsBeforeCallerID is greater than the number of rings defined by this parameter, the greater value is used.</li> </ul>
Web/EMS: Dialing Mode CLI: dialing-mode [IsTwoStageDial]	<p>Determines the dialing mode for IP-to-Tel (FXO) calls.</p> <ul style="list-style-type: none"> <li>[0] One Stage = One-stage dialing. In this mode, the device seizes one of the available lines (according to the ChannelSelectMode parameter), and then dials the destination phone number received in the INVITE message. To specify whether the dialing must start after detection of the dial tone or immediately after seizing the line, use the IsWaitForDialTone parameter.</li> <li>[1] Two Stages = (Default) Two-stage dialing. In this mode, the device seizes one of the PSTN/PBX lines without performing any dialing, connects the remote IP user to the PSTN/PBX, and all further signaling (dialing and Call Progress Tones) is performed directly with the PBX without the device's intervention.</li> </ul> <p><b>Note:</b> This parameter can also be configured in a Tel Profile.</p>
Web/EMS: Waiting For Dial Tone CLI: waiting-4-dial-tone [IsWaitForDialTone]	<p>Determines whether or not the device waits for a dial tone before dialing the phone number for IP-to-Tel (FXO) calls.</p> <ul style="list-style-type: none"> <li>[0] No</li> <li>[1] Yes (default)</li> </ul> <p>When one-stage dialing and this parameter are enabled, the device dials the phone number (to the PSTN/PBX line) only</p>

Parameter	Description
	<p>after it detects a dial tone. If this parameter is disabled, the device immediately dials the phone number after seizing the PSTN/PBX line without 'listening' for a dial tone.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The correct dial tone parameters must be configured in the CPT file.</li> <li>The device may take 1 to 3 seconds to detect a dial tone (according to the dial tone configuration in the CPT file). If the dial tone is not detected within 6 seconds, the device releases the call and sends a SIP 500 "Server Internal Error" response.</li> </ul>
Web: Time to Wait before Dialing [msec] EMS: Time Before Dial CLI: time-wait-b4-dialing <b>[WaitForDialTime]</b>	<p>For digital interfaces: Defines the delay after hook-flash is generated and until dialing begins. Applies to call transfer (i.e., the parameter TrunkTransferMode is set to 3) on CAS protocols.</p> <p>For analog interfaces: Defines the delay before the device starts dialing on the FXO line in the following scenarios:</p> <ul style="list-style-type: none"> <li>The delay between the time the line is seized and dialing begins during the establishment of an IP-to-Tel call. <b>Note:</b> Applicable only for one-stage dialing when the parameter IsWaitForDialTone is disabled.</li> <li>The delay between detection of a Wink and the start of dialing during the establishment of an IP-to-Tel call (for DID lines, EnableDIDWink is set to 1).</li> <li>For call transfer - the delay after hook-flash is generated and dialing begins.</li> </ul> <p>The valid range (in milliseconds) is 0 to 20,000 (i.e., 20 seconds). The default is 1,000 (i.e., 1 second).</p>
Web: Ring Detection Timeout [sec] EMS: Timeout Between Rings CLI: ring-detection-tout <b>[FXOBetweenRingTime]</b>	<p>Defines the timeout (in seconds) for detecting the second ring after the first detected ring.</p> <p>If automatic dialing is not used and Caller ID is enabled, the device seizes the line after detection of the second ring signal (allowing detection of caller ID sent between the first and the second rings). If the second ring signal is not received within this timeout, the device doesn't initiate a call to IP.</p> <p>If automatic dialing is used, the device initiates a call to IP when the ringing signal is detected. The FXO line is seized only if the remote IP party answers the call. If the remote party doesn't answer the call and the second ring signal is not received within this timeout, the device releases the IP call.</p> <p>This parameter is typically set to between 5 and 8. The default is 8.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only for Tel-to-IP calls.</li> <li>This timeout is calculated from the end of the ring until the start of the next ring. For example, if the ring cycle is two seconds on and four seconds off, the timeout value should be configured to five seconds (i.e., greater than the off time, e.g., four).</li> </ul>
Web: Rings before Detecting Caller	Determines the number of rings before the device starts

Parameter	Description
ID EMS: Rings Before Caller ID CLI: rings-b4-det-callerid <b>[RingsBeforeCallerID]</b>	detecting Caller ID. <ul style="list-style-type: none"> <li><b>[0]</b> 0 = Before first ring.</li> <li><b>[1]</b> 1 = (Default) After first ring.</li> <li><b>[2]</b> 2 = After second ring.</li> </ul>
Web/EMS: Guard Time Between Calls CLI: guard-time-btwn-calls <b>[GuardTimeBetweenCalls]</b>	Defines the time interval (in seconds) after a call has ended and a new call can be accepted for IP-to-Tel (FXO) calls. The valid range is 0 to 10. The default is 1. <b>Note:</b> Occasionally, after a call ends and on-hook is applied, a delay is required before placing a new call (and performing off-hook). This is necessary to prevent incorrect hook-flash detection or other glare phenomena.
Web: FXO Double Answer CLI: fxo-dbl-ans <b>[EnableFXODoubleAnswer]</b>	Enables the FXO Double Answer feature, which rejects (disconnects) incoming Tel (FXO)-to-IP collect calls and signals (informs) this call denial to the PSTN. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <b>Note:</b> This feature can also be configured in a Tel Profile.

## 59.11.12 Trunk Groups and Routing Parameters

The routing parameters are described in the table below.

### Routing Parameters

Parameter	Description
Trunk Group Table	
<b>Web:</b> Trunk Group Table EMS: SIP Endpoints > Phones CLI: configure voip > gw hunt-or-trunk-group TrunkGroup <b>[TrunkGroup]</b>	This table parameter configures and activates the device's endpoints/Trunk channels. This is done by defining telephone numbers and assigning them to Trunk Groups. The format of this parameter is shown below: <b>[TrunkGroup]</b> FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum, TrunkGroup_FirstTrunkId, TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel, TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId, TrunkGroup_LastTrunkId, TrunkGroup_Module; <b>[TrunkGroup]</b> For example: The configuration below assigns BRI channels 1 through 4 of Module 2 to Trunk Group ID 2 with phone numbers 208 to 211: TrunkGroup 1 = 2, 0, 1, 4, 208, 0, 0 ,2; <b>Notes:</b> <ul style="list-style-type: none"> <li>Trunk Group ID 1 is denoted as 0 in the table.</li> <li>This parameter can appear up to four times per module.</li> <li>For a description of this table, seeConfiguring Trunk Group Table on page 289.</li> </ul>
Hunt Group Settings	
Web: Hunt Group Settings EMS: SIP Routing > Hunt	This table parameter configures the rules for channel allocation per Trunk Group. The format of this parameter is as follows:

Parameter	Description
Group CLI: configure voip > gw hunt-or-trunk-group trunk- group-setting <b>[TrunkGroupSettings]</b>	<b>[TrunkGroupSettings]</b> FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId, TrunkGroupSettings_ChannelSelectMode, TrunkGroupSettings_RegistrationMode, TrunkGroupSettings_GatewayName, TrunkGroupSettings_ContactUser, TrunkGroupSettings_ServingIPGroup, TrunkGroupSettings_MWIInterrogationType, TrunkGroupSettings_TrunkGroupName; <b>[TrunkGroupSettings]</b> For example: TrunkGroupSettings 0 = 1, 0, 5, branch-hq, user, 1, 255, ; TrunkGroupSettings 1 = 2, 1, 0, localname, user1, 2, 255, ; <b>Note:</b> For a description of this table, see 'Configuring Hunt Group Settings' on page 291.
Web: Channel Select Mode EMS: Channel Selection Mode CLI: ch-select-mode <b>[ChannelSelectMode]</b>	Defines the method for allocating incoming IP-to-Tel calls to a channel for all Trunk Groups. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> By Dest Phone Number (default)</li> <li>▪ <b>[1]</b> Cyclic Ascending</li> <li>▪ <b>[2]</b> Ascending</li> <li>▪ <b>[3]</b> Cyclic Descending</li> <li>▪ <b>[4]</b> Descending</li> <li>▪ <b>[5]</b> Dest Number + Cyclic Ascending.</li> <li>▪ <b>[6]</b> By Source Phone Number</li> <li>▪ <b>[7]</b> Trunk Cyclic Ascending</li> <li>▪ <b>[8]</b> Trunk &amp; Channel Cyclic Ascending</li> <li>▪ <b>[9]</b> Ring to Hunt Group</li> <li>▪ <b>[10]</b> Select Trunk by ISDN SuppServ Table</li> <li>▪ <b>[11]</b> Dest Number + Ascending</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ For a detailed description of the parameter's options, see                'Configuring Hunt Group Settings' on page 291.</li> <li>▪ Channel select mode per Trunk Group can be configured in the                Hunt Group Settings (see 'Configuring Hunt Group Settings' on                page 291).</li> </ul>
Web: Default Destination Number CLI: dflt-dest-nb <b>[DefaultNumber]</b>	Defines the default destination phone number, which is used if the received message doesn't contain a called party number and no phone number is configured in the Trunk Group Table' (see Configuring the Trunk Group Table on page 289). This parameter is used as a starting number for the list of channels comprising all the device's Trunk Groups. The default is 1000.
Web: Source IP Address Input CLI: src-ip-addr-input <b>[SourceIPAddressInput]</b>	Determines which IP address the device uses to determine the source of incoming INVITE messages for IP-to-Tel routing. <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> = (Default) Auto Decision - if the IP-to-IP feature is enabled,                this parameter is automatically set to Layer 3 Source IP. If the IP-                to-IP feature is disabled, this parameter is automatically set to                SIP Contact Header (1).</li> <li>▪ <b>[0]</b> SIP Contact Header = The IP address in the Contact header</li> </ul>



Parameter	Description
	<p>of the incoming INVITE message is used.</p> <ul style="list-style-type: none"> <li><b>[1]</b> Layer 3 Source IP = The actual IP address (Layer 3) from where the SIP packet was received is used.</li> </ul>
Web: Use Source Number As Display Name EMS: Display Name CLI: src-nb-as-disp-name <b>[UseSourceNumberAsDisplayName]</b>	<p>Determines the use of Tel Source Number and Display Name for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) If a Tel Display Name is received, the Tel Source Number is used as the IP Source Number and the Tel Display Name is used as the IP Display Name. If no Display Name is received from the Tel side, the IP Display Name remains empty.</li> <li><b>[1]</b> Yes = If a Tel Display Name is received, the Tel Source Number is used as the IP Source Number and the Tel Display Name is used as the IP Display Name. If no Display Name is received from the Tel side, the Tel Source Number is used as the IP Source Number and also as the IP Display Name.</li> <li><b>[2]</b> Overwrite = The Tel Source Number is used as the IP Source Number and also as the IP Display Name (even if the received Tel Display Name is not empty).</li> <li><b>[3]</b> Original = Similar to option <b>[2]</b>, except that the operation is done before regular calling number manipulation.</li> </ul>
Web/EMS: Use Display Name as Source Number CLI: disp-name-as-src-nb <b>[UseDisplayNameAsSourceNumber]</b>	<p>Determines the use of Source Number and Display Name for IP-to-Tel calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) If IP Display Name is received, the IP Source Number is used as the Tel Source Number and the IP Display Name is used as the Tel Display Name. If no Display Name is received from IP, the Tel Display Name remains empty.</li> <li><b>[1]</b> Yes = If an IP Display Name is received, it is used as the Tel Source Number and also as the Tel Display Name, and Presentation is set to Allowed (0). If no Display Name is received from IP, the IP Source Number is used as the Tel Source Number and Presentation is set to Restricted (1).</li> </ul> <p>For example: When 'From: 100 &lt;sip:200@201.202.203.204&gt;' is received, the outgoing Source Number and Display Name are set to '100' and the Presentation is set to Allowed (0).  When 'From: &lt;sip:100@101.102.103.104&gt;' is received, the outgoing Source Number is set to '100' and the Presentation is set to Restricted (1).</p>
Web: Use Routing Table for Host Names and Profiles EMS: Use Routing Table For Host Names CLI: rte-tbl-4-host-names <b>[AlwaysUseRouteTable]</b>	<p>Determines whether to use the device's routing table to obtain the URI host name and optionally, an IP profile (per call) even if a Proxy server is used.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Don't use internal routing table.</li> <li><b>[1]</b> Enable = Use the Outbound IP Routing Table.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter appears only if the 'Use Default Proxy' parameter is enabled.</li> <li>The domain name is used instead of a Proxy name or IP address in the INVITE SIP URI.</li> </ul>
Web/EMS: Tel to IP Routing Mode CLI: tel2ip-rte-mode <b>[RouteModeTel2IP]</b>	<p>For a description of this parameter, see 'Configuring Outbound IP Routing Table' on page <a href="#">321</a>.</p>
<b>Outbound IP Routing Table</b>	



Parameter	Description
Web: Outbound IP Routing Table EMS: SIP Routing > Tel to IP CLI: configure voip > gw routing tel2ip-routing <b>[Prefix]</b>	This table parameter configures the Outbound IP Routing Table for routing Tel-to-IP and IP-to-IP calls. The format of this parameter is as follows: <b>[PREFIX]</b> FORMAT PREFIX_Index = PREFIX_DestinationPrefix, PREFIX_DestAddress, PREFIX_SourcePrefix, PREFIX_ProfileId, PREFIX_MeteringCode, PREFIX_DestPort, PREFIX_SrcIPGroupID, PREFIX_DestHostPrefix, PREFIX_DestIPGroupID, PREFIX_SrcHostPrefix, PREFIX_TransportType, PREFIX_SrcTrunkGroupID, PREFIX_DestSRD, PREFIX_CostGroup, PREFIX_ForkingGroup; <b>[PREFIX]</b> For example: PREFIX 0 = *, domain.com, *, 0, 255, \$\$, -1, , 1, , -1, -1, -1,;; PREFIX 1 = 20, 10.33.37.77, *, 0, 255, \$\$, -1, , 2, , 0, -1,;; <b>Note:</b> For a detailed description of this table, see 'Configuring Outbound IP Routing Table' on page 321.
<b>Inbound IP Routing Table</b>	
Web: Inbound IP Routing Table EMS: SIP Routing > IP to Hunt CLI: configure voip > gw routing ip2tel-routing <b>[PSTNPrefix]</b>	This table parameter configures the routing of IP-to-Trunk Groups (or inbound IP Groups). The format of this parameter is as follows: <b>[PSTNPrefix]</b> ORMAT PstnPrefix_Index = PstnPrefix_DestPrefix, PstnPrefix_TrunkGroupID, PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress, PstnPrefix_ProfileId, PstnPrefix_SrcIPGroupID, PstnPrefix_DestHostPrefix, PstnPrefix_SrcHostPrefix, PstnPrefix_SrcSRDID, PstnPrefix_TrunkId; <b>[PSTNPrefix]</b> For example: PstnPrefix 0 = 100, 1, 200, *, 0, 2, , , ,; PstnPrefix 1 = *, 2, *, , 1, 3, acl, joe, , ,; <b>Note:</b> For a detailed description of this table, see 'Configuring Inbound IP Routing Table' on page 330.
Web/EMS: IP to Tel Routing Mode CLI: ip2tel-rte-mode <b>[RouteModelIP2Tel]</b>	Determines whether to route IP calls to the Trunk Group (or IP Group) before or after manipulation of the destination number (configured in 'Configuring Source/Destination Number Manipulation Rules' on page 297). <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Route calls before manipulation = (Default) Calls are routed before the number manipulation rules are applied.</li> <li>▪ <b>[1]</b> Route calls after manipulation = Calls are routed after the number manipulation rules are applied.</li> </ul>
Web: IP Security EMS: Secure Call From IP CLI: ip-security <b>[SecureCallsFromIP]</b>	Determines the device's policy on accepting or blocking SIP calls (IP-to-Tel calls). This is useful in preventing unwanted SIP calls, SIP messages, and/or VoIP spam. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) The device accepts all SIP calls.</li> <li>▪ <b>[1]</b> Secure Incoming calls = The device accepts SIP calls (i.e., calls from the IP side) only from IP addresses that are defined in the Outbound IP Routing Table or Proxy Set table, or IP addresses resolved from DNS servers from FQDN values defined in the Proxy Set table. All other incoming calls are rejected.</li> <li>▪ <b>[2]</b> Secure All calls = The device accepts SIP calls only from IP</li> </ul>

Parameter	Description
	<p>addresses (in dotted-decimal notation format) that are defined in the Outbound IP Routing Table table or Proxy Set table, and rejects all other incoming calls. In addition, if an FQDN is defined in the routing table or Proxy Set table, the call is allowed to be sent only if the resolved DNS IP address appears in one of these tables; otherwise, the call is rejected. Therefore, the difference between this option and option <b>[1]</b> is that this option is concerned only about numerical IP addresses that are defined in the tables.</p> <p><b>Note:</b> If this parameter is set to <b>[1]</b> or <b>[2]</b>, when using Proxies or Proxy Sets, it is unnecessary to configure the Proxy IP addresses in the routing table. The device allows SIP calls received from the Proxy IP addresses even if these addresses are not configured in the routing table.</p>
Web/EMS: Filter Calls to IP CLI: filter-calls-to-ip <b>[FilterCalls2IP]</b>	<p>Enables filtering of Tel-to-IP calls when a Proxy is used (i.e., IsProxyUsed parameter is set to 1 - see 'Configuring Proxy and Registration Parameters' on page 222).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Don't Filter = (Default) The device doesn't filter calls when using a Proxy.</li> <li><b>[1]</b> Filter = Filtering is enabled.</li> </ul> <p>When this parameter is enabled and a Proxy is used, the device first checks the Outbound IP Routing Table before making a call through the Proxy. If the number is not allowed (i.e., number isn't listed in the table or a call restriction routing rule of IP address 0.0.0.0 is applied), the call is released.</p> <p><b>Note:</b> When no Proxy is used, this parameter must be disabled and filtering is according to the Outbound IP Routing Table.</p>
CLI: ip2tel-tagging-dst <b>[IP2TelTaggingDestDialPlanIndex]</b>	<p>Determines the Dial Plan index in the external Dial Plan file (.dat) in which string labels ("tags") are defined for tagging incoming IP-to-Tel calls. The special "tag" is added as a prefix to the called party number, and then the Inbound IP Routing Table uses this "tag" instead of the original prefix. Manipulation is then performed (after routing) in the Manipulation table which strips the "tag" characters before sending the call to the endpoint.</p> <p>The valid values are 0 to 7, where 0 denotes PLAN1, 1 denotes PLAN2, and so on. The default is -1 (i.e., no dial plan file used). The routing label can be up to 9 (text) characters.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to digital interfaces.</li> <li>The routing must be configured to be performed before manipulation.</li> <li>For more information on this feature, see Dial Plan Prefix Tags for IP-to-Tel Routing on page 544.</li> </ul>
CLI: etsi-diversion <b>[EnableETSIDiversion]</b>	<p>Determines the method in which the Redirect Number is sent to the Tel side.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Q.931 Redirecting Number Information Element (IE).</li> <li><b>[1]</b> = ETSI DivertingLegInformation2 in a Facility IE.</li> </ul>
Web: Add CIC CLI: add-cic <b>[AddCicAsPrefix]</b>	<p>Determines whether to add the Carrier Identification Code (CIC) as a prefix to the destination phone number for IP-to-Tel calls. When this parameter is enabled, the 'cic' parameter in the incoming SIP INVITE can be used for IP-to-Tel routing decisions. It routes the call to the appropriate Trunk Group based on this parameter's value.</p>

Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> No (default)</li> <li>▪ <b>[1]</b> Yes</li> </ul> <p>For digital interfaces: The SIP 'cic' parameter enables the transmission of the 'cic' parameter from the SIP network to the ISDN. The 'cic' parameter is a three- or four-digit code used in routing tables to identify the network that serves the remote user when a call is routed over many different networks. The 'cic' parameter is carried in the SIP INVITE and maps to the ISDN Transit Network Selection Information Element (TNS IE) in the outgoing ISDN Setup message (if the EnableCIC parameter is set to 1). The TNS IE identifies the requested transportation networks and allows different providers equal access support, based on customer choice.</p> <p>For example, as a result of receiving the below INVITE, the destination number after number manipulation is cic+167895550001: INVITE sip:5550001;cic=+16789@172.18.202.60:5060;user=phone SIP/2.0</p> <p><b>Note:</b> After the cic prefix is added, the Inbound IP Routing Table can be used to route this call to a specific Trunk Group. The Destination Number IP to Tel Manipulation table must be used to remove this prefix before placing the call to the ISDN.</p>
<b>[FaxReroutingMode]</b>	<p>Enables re-routing of Tel-to-IP calls that are identified as fax calls. If a CNG tone is detected on the Tel side of a Tel-to-IP call, the prefix string "FAX" is appended to the destination number before routing and manipulation. If you enter the string value, "FAX" as the destination number in the Outbound IP Routing table, the routing rule is used to route the call and the destination number manipulation mechanism is used to remove the "FAX" prefix, if required. Note that the "FAX" prefix string in routing and manipulation tables is case-sensitive.</p> <p>If the initial INVITE used to establish the voice call (not fax) was already sent, a CANCEL (if not connected yet) or a BYE (if already connected) is sent to release the voice call.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Rerouting without Delay</li> <li>▪ <b>[2]</b> Progress and Delay = Incoming ISDN calls are delayed until a CNG tone detection or timeout, set by the FaxReroutingDelay parameter. If the EnableComfortTone parameter is set to 1, a Q.931 Progress message with Protocol Discriminator set to 1 is sent to the PSTN and a comfort tone is played accordingly to the PSTN. When the timeout expires, the device sends an INVITE to a specific IP Group or to a fax server, according to the Outbound IP Routing table rules. This option is applicable only to ISDN.</li> <li>▪ <b>[3]</b> Connect and Delay = Incoming ISDN calls are delayed until a CNG tone detection or timeout, set by the FaxReroutingDelay parameter. A Q.931 Connect message is sent to the PSTN. If the EnableComfortTone parameter is set to 1, a comfort tone is played to the PSTN. When the timeout expires, the device sends an INVITE to a specific IP Group or to a fax server according to the Outbound IP Routing table rules. This option is applicable only to ISDN.</li> </ul> <p><b>Note:</b> This parameter has replaced the EnableFaxRerouting parameter. For backward compatibility, the EnableFaxRerouting parameter set to 1 is equivalent to the FaxReroutingMode parameter</p>

Parameter	Description
	set to 1.
<b>[FaxReroutingDelay]</b>	<p>Defines the maximum time interval (in seconds) that the device waits for CNG detection before re-routing calls identified as fax calls to fax destinations (terminating fax machine).</p> <p>The valid value range is 1-10. The default is 5.</p>
Web: ENUM Resolution CLI: enum-service-domain <b>[EnumService]</b>	<p>Defines the ENUM service for translating telephone numbers to IP addresses or domain names (FQDN). For example, e164.arpa, e164.customer.net, or NRENum.net.</p> <p>The valid value is a string of up to 50 characters. The default is "e164.arpa".</p> <p><b>Note:</b> ENUM-based routing is configured in the Outbound IP Routing table using the "ENUM" string value as the destination address to denote this parameter's value.</p>

### 59.11.13 IP Connectivity Parameters

The IP connectivity parameters are described in the table below.

**IP Connectivity Parameters**

Parameter	Description
Web: Enable Alt Routing Tel to IP EMS: Enable Alternative Routing CLI: alt-routing-tel2ip <b>[AltRoutingTel2IPEnable]</b>	<p>Enables the Alternative Routing feature for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Disables the Alternative Routing feature.</li> <li><b>[1]</b> Enable = Enables the Alternative Routing feature.</li> <li><b>[2]</b> Status Only = The Alternative Routing feature is disabled, but read-only information on the QoS of the destination IP addresses is provided.</li> </ul>
Web: Alt Routing Tel to IP Mode EMS: Alternative Routing Mode CLI: alt-rte-tel2ip-mode <b>[AltRoutingTel2IPMode]</b>	<p>Determines the IP Connectivity event(s) reason for triggering Alternative Routing.</p> <ul style="list-style-type: none"> <li><b>[0]</b> None = Alternative routing is not used.</li> <li><b>[1]</b> Connectivity = Alternative routing is performed if SIP OPTIONS message to the initial destination fails (determined according to the AltRoutingTel2IPConnMethod parameter).</li> <li><b>[2]</b> QoS = Alternative routing is performed if poor QoS is detected.</li> <li><b>[3]</b> Both = (Default) Alternative routing is performed if either SIP OPTIONS to initial destination fails, poor QoS is detected, or the DNS host name is not resolved.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>QoS is quantified according to delay and packet loss calculated according to previous calls. QoS statistics are reset if no new data is received within two minutes.</li> <li>To receive quality information (displayed in the 'Quality Status' and 'Quality Info.' fields in 'Viewing IP Connectivity' on page 597) per destination, this parameter must be set to 2 or 3.</li> </ul>
Web: Alt Routing Tel to IP Connectivity Method EMS: Alternative Routing Telephone to IP Connection Method CLI: alt-rte-tel2ip-method	<p>Determines the method used by the device for periodically querying the connectivity status of a destination IP address.</p> <ul style="list-style-type: none"> <li><b>[0]</b> ICMP Ping = (Default) Internet Control Message Protocol (ICMP) ping messages.</li> <li><b>[1]</b> SIP OPTIONS = The remote destination is considered offline if</li> </ul>

Parameter	Description
<b>[AltRoutingTel2IPConnMethod]</b>	the latest OPTIONS transaction timed out. Any response to an OPTIONS request, even if indicating an error, brings the connectivity status to online. <b>Note:</b> ICMP Ping is currently not supported for the IP Connectivity feature.
Web: Alt Routing Tel to IP Keep Alive Time EMS: Alternative Routing Keep Alive Time CLI: alt-rte-tel2ip-keep-alive <b>[AltRoutingTel2IPKeepAliveTime]</b>	Defines the time interval (in seconds) between SIP OPTIONS Keep-Alive messages used for the IP Connectivity application. The valid range is 5 to 2,000,000. The default is 60.
Web: Max Allowed Packet Loss for Alt Routing [%] CLI: mx-pkt-loss-4-alt-rte <b>[IPConnQoSMaxAllowedPL]</b>	Defines the packet loss (in percentage) at which the IP connection is considered a failure and Alternative Routing mechanism is activated. The default is 20%.
Web: Max Allowed Delay for Alt Routing [msec] CLI: mx-all-dly-4-alt-rte <b>[IPConnQoSMaxAllowedDelay]</b>	Defines the transmission delay (in msec) at which the IP connection is considered a failure and the Alternative Routing mechanism is activated. The range is 100 to 10,000. The default is 250.

### 59.11.14 Alternative Routing Parameters

The alternative routing parameters are described in the table below.

**Alternative Routing Parameters**

Parameter	Description
Web/EMS: Redundant Routing Mode CLI: redundant-routing-m <b>[RedundantRoutingMode]</b>	Determines the type of redundant routing mechanism when a call can't be completed using the main route. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = No redundant routing is used. If the call can't be completed using the main route (using the active Proxy or the first matching rule in the Routing table), the call is disconnected.</li> <li><b>[1]</b> Routing Table = (Default) Internal routing table is used to locate a redundant route.</li> <li><b>[2]</b> Proxy = Proxy list is used to locate a redundant route.</li> </ul> <b>Note:</b> To implement the Redundant Routing Mode mechanism, you first need to configure the parameter AltRouteCauseTEL2IP (Reasons for Alternative Routing table).
<b>[EnableAltMapTel2IP]</b>	Enables different Tel-to-IP destination number manipulation rules per routing rule when several (up to three) Tel-to-IP routing rules are defined and if alternative routing using release causes is used. For example, if an INVITE message for a Tel-to-IP call is returned with a SIP 404 Not Found response, the call can be re-sent to a different destination number (as defined using the parameter NumberMapTel2IP). <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li><b>[1]</b> = Enable</li> </ul>
Web/EMS: Alternative Routing Tone Duration <b>[ms]</b> CLI: alt-rte-tone-duration <b>[AltRoutingToneDuration]</b>	<p>Defines the duration (in milliseconds) for which the device plays a tone to the endpoint on each attempt for Tel-to-IP alternative routing. When the device finishes playing the tone, a new SIP INVITE message is sent to the new IP destination. The tone played is the call forward tone (Tone Type #25 in the CPT file).</p> <p>The valid range is 0 to 20,000. The default is 0 (i.e., no tone is played).</p> <p><b>Note:</b> This parameter is applicable only to Tel-to-IP alternative routing.</p>
<b>Reasons for Alternative Tel-to-IP Routing Table</b>	
Web: Reasons for Alternative Routing EMS: Alt Route Cause Tel to IP CLI: configure voip > gw manipulations general-setting alt-route-cause-tel2ip <b>[AltRouteCauseTel2IP]</b>	<p>This table parameter configures SIP call failure reason values received from the IP side. If an IP call is released as a result of one of these reasons, the device attempts to locate an alternative IP route for the call in the Outbound IP Routing Table (if a Proxy is not used) or used as a redundant Proxy (you need to set the parameter RedundantRoutingMode to 2). The release reason for Tel-to-IP calls is provided in SIP 4xx, 5xx, and 6xx response codes.</p> <p>The format of this parameter is as follows:</p> <p><b>[AltRouteCauseTel2IP]</b>  FORMAT AltRouteCauseTel2IP_Index =  AltRouteCauseTel2IP_ReleaseCause;  <b>[AltRouteCauseTel2IP]</b></p> <p>For example:  AltRouteCauseTel2IP 0 = 486; (Busy Here)  AltRouteCauseTel2IP 1 = 480; (Temporarily Unavailable)  AltRouteCauseTel2IP 2 = 408; (No Response)</p> <p><b>Note:</b> For a detailed description of this table, see 'Alternative Routing Based on SIP Responses' on page <a href="#">336</a>.</p>
<b>Reasons for Alternative IP-to-Tel Routing Table</b>	
Web: Reasons for Alternative IP-to-Tel Routing EMS: Alt Route Cause IP to Tel CLI: configure voip > gw manipulations general-setting alt-route-cause-ip2tel <b>[AltRouteCauseIP2Tel]</b>	<p>This table parameter configures call failure reason values received from the PSTN side (in Q.931 presentation). If a call is released as a result of one of these reasons, the device attempts to locate an alternative Trunk Group for the call in the Inbound IP Routing Table.</p> <p>The format of this parameter is as follows:</p> <p><b>[AltRouteCauseIP2Tel]</b>  FORMAT AltRouteCauseIP2Tel_Index =  AltRouteCauseIP2Tel_ReleaseCause;  <b>[AltRouteCauseIP2Tel]</b></p> <p>For example:  AltRouteCauseIP2Tel 0 = 3 (No Route to Destination)  AltRouteCauseIP2Tel 1 = 1 (Unallocated Number)  AltRouteCauseIP2Tel 2 = 17 (Busy Here)  AltRouteCauseIP2Tel 2 = 27 (Destination Out of Order)</p> <p><b>Note:</b> For a detailed description of this table, see 'Alternative Routing to Trunk upon Q.931 Call Release Cause Code' on page <a href="#">339</a>.</p>
<b>Forward On Busy Trunk Destination Table</b>	
Web/EMS: Forward On Busy Trunk Destination CLI: configure voip > gw routing fwd-on-bsy-trk-dest	<p>This table parameter configures the Forward On Busy Trunk Destination table. This table allows you to define an alternative IP destination if a trunk is busy for IP-to-Tel calls.</p> <p>The format of this parameter is as follows:</p>



Parameter	Description
<b>[ForwardOnBusyTrunkDest]</b>	<p><b>[ForwardOnBusyTrunkDest]</b>            FORMAT ForwardOnBusyTrunkDest_Index =            ForwardOnBusyTrunkDest_TrunkGroupId,            ForwardOnBusyTrunkDest_ForwardDestination;  <b>[ForwardOnBusyTrunkDest]</b></p> <p>For example, the below configuration forwards IP-to-Tel calls to destination user "112" at host IP address 10.13.4.12, port 5060, using transport protocol TCP, if Trunk Group ID 2 is unavailable:            ForwardOnBusyTrunkDest 1 = 2,            112@10.13.4.12:5060;transport=tcp;</p> <p><b>Note:</b> For a detailed description of this table, see 'Alternative Routing to IP Destination upon Busy Trunk' on page 340.</p>

### 59.11.15 Number Manipulation Parameters

The number manipulation parameters are described in the table below.

**Number Manipulation Parameters**

Parameter	Description
<b>[ManipulateIP2PSTNReferTo]</b>	<p>Enables the manipulation of the called party (destination) number according to the SIP Refer-To header received by the device for TDM (PSTN) blind transfer. The number in the SIP Refer-To header is manipulated for all types of blind transfers to the PSTN (TBCT, ECT, RLT, QSIG, FXO, and CAS).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>During the blind transfer, the device initiates a new call to the PSTN and the destination number of this call can be manipulated if this parameter is enabled. When enabled, the manipulation is done as follows:</p> <ol style="list-style-type: none"> <li>1 If you configure a value for the xferPrefix parameter, then this value (string) is added as a prefix to the number in the Refer-To header.</li> <li>2 This called party number is then manipulated using the IP-to-Tel Destination Phone Number Manipulation table. The source number of the transferred call is taken from the original call, according to its initial direction:               <ul style="list-style-type: none"> <li>✓ Source number of the original call if it is a Tel-to-IP call</li> <li>✓ Destination number of the original call if it is an IP-to-Tel call</li> </ul> <p>This source number can also be used as the value for the 'Source Prefix' field in the IP-to-Tel Destination Phone Number Manipulation table. The local IP address is used as the value for the 'Source IP Address' field.</p> </li> </ol> <p><b>Note:</b> This manipulation does not affect IP-to-Trunk Group routing rules.</p>

Parameter	Description
Web: Use EndPoint Number As Calling Number Tel2IP EMS: Use EP Number As Calling Number Tel to IP CLI: epn-as-cpn-tel2ip <b>[UseEPNumAsCallingNumTel2IP]</b>	<p>Enables the use of the B-channel number as the calling number (sent in the From field of the INVITE) instead of the number received in the Q.931 Setup message, for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>For example, if the incoming calling party number in the Q.931 Setup message is "12345" and the B-channel number is 17, then the outgoing INVITE From header is set to "17" instead of "12345".</p> <p><b>Note:</b> When enabled, this feature is applied before routing and manipulation on the source number.</p>
Web: Use EndPoint Number As Calling Number IP2Tel EMS: Use EP Number As Calling Number IP to Tel CLI: epn-as-cpn-ip2tel <b>[UseEPNumAsCallingNumIP2Tel]</b>	<p>Enables the use of the B-channel number as the calling party number (sent in the Q.931 Setup message) instead of the number received in the From header of the INVITE, for IP-to-Tel calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>For example, if the incoming INVITE From header contains "12345" and the destined B-channel number is 17, then the outgoing calling party number in the Q.931 Setup message is set to "17" instead of "12345".</p> <p><b>Note:</b> When enabled, this feature is applied after routing and manipulation on the source number (i.e., just before sending to the Tel side).</p>
Web: Tel2IP Default Redirect Reason CLI: tel-to-ip-dflt-redir-rsn <b>[Tel2IPDefaultRedirectReason]</b>	<p>Determines the default redirect reason for Tel-to-IP calls when no redirect reason (or "unknown") exists in the received Q931 ISDN Setup message. The device includes this default redirect reason in the SIP History-Info header of the outgoing INVITE.</p> <p>If a redirect reason exists in the received Setup message, this parameter is ignored and the device sends the INVITE message with the reason according to the received Setup message. If this parameter is not configured (-1), the outgoing INVITE is sent with the redirect reason as received in the Setup message (if none or "unknown" reason, then without a reason).</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured = (Default) Received redirect reason is not changed</li> <li>▪ <b>[1]</b> Busy = Call forwarding busy</li> <li>▪ <b>[2]</b> No Reply = Call forwarding no reply</li> <li>▪ <b>[9]</b> DTE Out of Order = Call forwarding DTE out of order</li> <li>▪ <b>[10]</b> Deflection = Call deflection</li> <li>▪ <b>[15]</b> Systematic/Unconditional = Call forward unconditional</li> </ul>
Web: Redirect Number SIP to TEL EMS: Set IP To Tel Redirect Screening Indicator CLI: redir-nb-si-2tel <b>[SetIp2TelRedirectScreeningInd]</b>	<p>Determines the value of the Redirect Number screening indicator in ISDN Setup messages.</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured (default)</li> <li>▪ <b>[0]</b> User Provided</li> <li>▪ <b>[1]</b> User Passed</li> <li>▪ <b>[2]</b> User Failed</li> <li>▪ <b>[3]</b> Network Provided</li> </ul> <p><b>Note:</b> This parameter is applicable only to digital PSTN interfaces (ISDN).</p>



Parameter	Description
Web: Set IP-to-TEL Redirect Reason CLI: ip2tel-redir-reason <b>[SetIp2TelRedirectReason]</b>	Defines the redirect reason for IP-to-Tel calls. If redirect (diversion) information is received from the IP, the redirect reason is set to the value of this parameter before the device sends it on to the Tel. <ul style="list-style-type: none"> <li>▪ [-1] Not Configured (default)</li> <li>▪ [0] Unkown</li> <li>▪ [1] Busy</li> <li>▪ [2] No Reply</li> <li>▪ [3] Network Busy</li> <li>▪ [4] Deflection</li> <li>▪ [9] DTE out of Order</li> <li>▪ [10] Forwarding DTE</li> <li>▪ [13] Transfer</li> <li>▪ [14] Pickup</li> <li>▪ [15] Systematic/Unconditional</li> </ul> <b>Note:</b> This parameter is applicable only to digital PSTN interfaces (ISDN).
Web: Set TEL-to-IP Redirect Reason CLI: tel2ip-redir-reason <b>[SetTel2IpRedirectReason]</b>	Defines the redirect reason for Tel-to-IP calls. If redirect (diversion) information is received from the Tel, the redirect reason is set to the value of this parameter before the device sends it on to the IP. <ul style="list-style-type: none"> <li>▪ [-1] Not Configured (default)</li> <li>▪ [0] Unkown</li> <li>▪ [1] Busy</li> <li>▪ [2] No Reply</li> <li>▪ [3] Network Busy</li> <li>▪ [4] Deflection</li> <li>▪ [9] DTE out of Order</li> <li>▪ [10] Forwarding DTE</li> <li>▪ [13] Transfer</li> <li>▪ [14] Pickup</li> <li>▪ [15] Systematic/Unconditional</li> </ul> <b>Note:</b> This parameter is applicable only to digital PSTN interfaces (ISDN).
Web: Send Screening Indicator to IP EMS: Screening Indicator To IP <b>[ScreeningInd2IP]</b>	Overrides the calling party's number (CPN) screening indication in the received ISDN SETUP message for Tel-to-IP calls. <ul style="list-style-type: none"> <li>▪ [-1] Not Configured = (Default) Not configured (interworking from ISDN to IP) or set to 0 for CAS.</li> <li>▪ [0] User Provided = CPN set by user, but not screened (verified).</li> <li>▪ [1] User Passed = CPN set by user, verified and passed.</li> <li>▪ [2] User Failed = CPN set by user, and verification failed.</li> <li>▪ [3] Network Provided = CPN set by network.</li> </ul> <b>Note:</b> This parameter is applicable only if the Remote Party ID (RPID) header is enabled.

Parameter	Description
Web: Send Screening Indicator to ISDN EMS: Screening Indicator To ISDN <b>[ScreeningInd2ISDN]</b>	<p>Overrides the screening indicator of the calling party's number for IP-to-Tel ISDN calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured = (Default) Not configured (interworking from IP to ISDN).</li> <li>▪ <b>[0]</b> User Provided = user provided, not screened.</li> <li>▪ <b>[1]</b> User Passed = user provided, verified and passed.</li> <li>▪ <b>[2]</b> User Failed = user provided, verified and failed.</li> <li>▪ <b>[3]</b> Network Provided = network provided</li> </ul> <p><b>Note:</b> This parameter is applicable only to digital PSTN interfaces (ISDN).</p>
Web: Copy Destination Number to Redirect Number EMS: Copy Dest to Redirect Number CLI: cp-dst-nb-2-redir-nb <b>[CopyDest2RedirectNumber]</b>	<p>Determines whether the device copies the received ISDN (digital interfaces) called number to the outgoing SIP Diversion header for Tel-to-IP calls (even if a Redirecting Number IE is not received in the ISDN Setup message, for digital interfaces). Therefore, the called number is used as a redirect number. Call redirection information is typically used for Unified Messaging and voice mail services to identify the recipient of a message.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Don't copy = (Default) Disable.</li> <li>▪ <b>[1]</b> Copy after phone number manipulation = Copies the called number after manipulation. The device first performs Tel-to-IP destination phone number manipulation (i.e., on the SIP To header), and only then copies the manipulated called number to the SIP Diversion header for the Tel-to-IP call. Therefore, with this option, the called and redirect numbers are identical.</li> <li>▪ <b>[2]</b> Copy before phone number manipulation = Copies the called number before manipulation. The device first copies the original called number to the SIP Diversion header, and then performs Tel-to-IP destination phone number manipulation. Therefore, this allows you to have different numbers for the called (i.e., SIP To header) and redirect (i.e., SIP Diversion header) numbers.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For digital interfaces: If the incoming ISDN-to-IP call includes a Redirect Number, this number is overridden by the new called number if this parameter is set to <b>[1]</b> or <b>[2]</b>.</li> <li>▪ When configured in an IP Profile, this parameter can also be used for IP-to-Tel calls. The device can overwrite the redirect number with the destination number from the received SIP INVITE message in the outgoing ISDN call. This is achieved by assigning an IP Profile (IPProfile parameter) defined with the CopyDest2RedirectNumber parameter set to 1, to the IP-to-Tel Routing table (PSTNPrefix parameter). Even if there is no SIP Diversion or History header in the incoming INVITE message, the outgoing Q.931 Setup message will contain a redirect number.</li> <li>▪ This parameter can also be configured in an IP Profile.</li> </ul>
CLI: rep-calling-w-redir disc-on-bsy-tone-i <b>[ReplaceCallingWithRedirectNumber]</b>	<p>Enables the replacement of the calling number with the redirect number for ISDN-to-IP calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = The calling name is removed and left blank. The outgoing INVITE message excludes the redirect number that was used to replace the calling number. The replacement is done only if a redirect number is present in the incoming Tel call.</li> <li>▪ <b>[2]</b> = Manipulation is done on the new calling party number (after manipulation of the original calling party number, using the</li> </ul>

Parameter	Description
	<p>Tel2IPSourceNumberMappingDialPlanIndex parameter), but before the regular calling or redirect number manipulation:</p> <ul style="list-style-type: none"> <li>✓ If a redirect number exists, it replaces the calling party number. If there is no redirect number, the calling number is left unchanged.</li> <li>✓ If there is a calling "display" name, it remains unchanged.</li> <li>✓ The redirect number remains unchanged and is included in the SIP Diversion header.</li> </ul>
<p>Web/EMS: Add Trunk Group ID as Prefix CLI: trkgripid-prefix <b>[AddTrunkGroupAsPrefix]</b></p>	<p>Determines whether the Trunk Group ID is added as a prefix to the destination phone number (i.e., called number) for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No = (Default) Don't add Trunk Group ID as prefix.</li> <li>▪ <b>[1]</b> Yes = Add Trunk Group ID as prefix to called number.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This option can be used to define various routing rules.</li> <li>▪ To use this feature, you must configure the Trunk Group IDs (see Configuring Trunk Group Table on page 289).</li> </ul>
<p>Web: Add Trunk ID as Prefix EMS: Add Port ID As Prefix CLI: trk-id-as-prefix <b>[AddPortAsPrefix]</b></p>	<p>Determines whether or not the port number / Trunk ID is added as a prefix to the called (destination) number for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No (Default)</li> <li>▪ <b>[1]</b> Yes</li> </ul> <p>If enabled, the device adds the following prefix to the called phone number: slot number (a single digit in the range of 1 to 6) and port number / Trunk ID (single digit in the range 1 to 8). For example, for the first trunk/channel located in the first slot, the number "11" is added as the prefix.</p> <p>This option can be used to define various routing rules.</p>
<p>Web/EMS: Add Trunk Group ID as Prefix to Source CLI: trkgripid-pref2source <b>[AddTrunkGroupAsPrefix ToSource]</b></p>	<p>Determines whether the device adds the Trunk Group ID (from where the call originated) as the prefix to the calling number (i.e. source number).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No (default)</li> <li>▪ <b>[1]</b> Yes</li> </ul>
<p>Web: Replace Empty Destination with B-channel Phone Number EMS: Replace Empty Dst With Port Number CLI: empty-dst-w-bch-nb <b>[ReplaceEmptyDstWithPortNumber]</b></p>	<p>Determines whether the internal channel number is used as the destination number if the called number is missing.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No (default)</li> <li>▪ <b>[1]</b> Yes</li> </ul> <p><b>Note:</b> This parameter is applicable only to Tel-to-IP calls and if the called number is missing.</p>
<p><b>[CopyDestOnEmptySource]</b></p>	<p>Determines whether the destination number is copied to the source number if no source number is present, for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Source Number is left empty.</li> <li>▪ <b>[1]</b> = If the Source Number of a Tel-to-IP call is empty, the Destination Number is copied to the Source Number.</li> </ul>
<p>Web: Add NPI and TON to Calling Number EMS: Add NPI And TON As Prefix To Calling Number CLI: npi-n-ton-to-cng-nb</p>	<p>Determines whether the Numbering Plan Indicator (NPI) and Type of Numbering (TON) are added to the Calling Number for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No = (Default) Do not change the Calling Number.</li> <li>▪ <b>[1]</b> Yes = Add NPI and TON to the Calling Number ISDN Tel-to-IP</li> </ul>

Parameter	Description
<b>[AddNPIandTON2CallingNumber]</b>	<p>call.</p> <p>For example: After receiving a Calling Number of 555, NPI of 1, and TON of 3, the modified number becomes 13555. This number can later be used for manipulation and routing.</p>
Web: Add NPI and TON to Called Number EMS: Add NPI And TON As Prefix To Called Number CLI: np-n-ton-to-cld-nb <b>[AddNPIandTON2CalledNumber]</b>	<p>Determines whether NPI and TON are added to the Called Number for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) Do not change the Called Number.</li> <li><b>[1]</b> Yes = Add NPI and TON to the Called Number of ISDN Tel-to-IP call.</li> </ul> <p>For example: After receiving a Called Number of 555, NPI of 1 and TON of 3, the modified number becomes 13555. This number can later be used for manipulation and routing.</p>
Web: Add NPI and TON to Redirect Number CLI: np-n-ton-2-redirnb <b>[AddNPIandTON2RedirectNumber]</b>	<p>Determines whether the NPI and TON values are added as the prefix to the Redirect number in INVITE messages' Diversion or History-Info headers, for ISDN Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Yes (Default)</li> <li><b>[1]</b> No</li> </ul>
Web: IP to Tel Remove Routing Table Prefix EMS: Remove Prefix CLI: ip2tel-rmv-rte-tbl <b>[RemovePrefix]</b>	<p>Determines whether or not the device removes the prefix (as configured in the Inbound IP Routing Table - see 'Configuring Inbound IP Routing Table' on page 330) from the destination number for IP-to-Tel calls, before sending it to the Tel.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No (default)</li> <li><b>[1]</b> Yes</li> </ul> <p>For example: To route an incoming IP-to-Tel call with destination number "21100", the Inbound IP Routing Table is scanned for a matching prefix. If such a prefix is found (e.g., "21"), then before the call is routed to the corresponding Trunk Group, the prefix "21" is removed from the original number, and therefore, only "100" remains.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only if number manipulation is performed after call routing for IP-to-Tel calls (i.e., RouteModelP2Tel parameter is set to 0).</li> <li>Similar operation (of removing the prefix) is also achieved by using the usual number manipulation rules.</li> </ul>
Web/EMS: Swap Redirect and Called Numbers CLI: swap-rdr-n-called-nb <b>[SwapRedirectNumber]</b>	<ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) Don't change numbers.</li> <li><b>[1]</b> Yes = Incoming ISDN call that includes a redirect number (sometimes referred to as 'original called number') uses the redirect number instead of the called number.</li> </ul>
<b>[UseReferredByForCallingNumber]</b>	<p>Determines whether the device uses the number from the URI in the SIP Referred-By header as the calling number in the outgoing Q.931 Setup message, when SIP REFER messages are received.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) No</li> <li><b>[1]</b> = Yes</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable to all ISDN (TBCT, RLT, ECT) and CAS blind call transfers (except for in-band) and when the device receives SIP REFER messages with a Referred-By header.</li> <li>This manipulation is done before regular IP-to-Tel source number manipulation.</li> </ul>

Parameter	Description
<b>[SwapTel2IPCalled&amp;CallingNumbers]</b>	<p>Determines whether the device swaps the calling and called numbers received from the Tel side (for Tel-to-IP calls). The SIP INVITE message contains the swapped numbers.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disabled</li> <li><b>[1]</b> = Swap calling and called numbers</li> </ul> <p><b>Note:</b> This parameter can also be configured in a Tel Profile.</p>
Web/EMS: Add Prefix to Redirect Number CLI: add-pref-to-redir-nb <b>[Prefix2RedirectNumber]</b>	<p>Defines a string prefix that is added to the Redirect number received from the Tel side. This prefix is added to the Redirect Number in the SIP Diversion header.</p> <p>The valid range is an 8-character string. The default is an empty string.</p>
Web: Add Number Plan and Type to RPI Header EMS: Add Ton 2 RPI CLI: np-n-type-to-rpi-hdr <b>[AddTON2RPI]</b>	<p>Determines whether the TON/PLAN parameters are included in the Remote-Party-ID (RPID) header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No</li> <li><b>[1]</b> Yes (default)</li> </ul> <p>If the Remote-Party-ID header is enabled (EnableRPIHeader = 1) and AddTON2RPI = 1, it's possible to configure the calling and called number type and number plan using the Number Manipulation tables for Tel-to-IP calls.</p>
Web/EMS: Source Manipulation Mode CLI: src-manipulation <b>[SourceManipulationMode]</b>	<p>Determines the SIP headers containing the source number after manipulation:</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) The SIP From and P-Asserted-Identity headers contain the source number after manipulation.</li> <li><b>[1]</b> = Only SIP From header contains the source number after manipulation, while the P-Asserted-Identity header contains the source number before manipulation.</li> </ul>
<b>Calling Name Manipulations IP-to-Tel Table</b>	
CLI: configure voip > gw manipulations calling-name-map-ip2tel <b>[CallingNameMapIp2Tel]</b>	<p>Configures rules for manipulating the calling name (caller ID) in the received SIP message for IP-to-Tel calls. This can include modifying or removing the calling name. The format of this table ini file parameter is as follows:</p> <p><b>[ CallingNameMapIp2Tel ]</b>            FORMAT CallingNameMapIp2Tel_Index =            CallingNameMapIp2Tel_DestinationPrefix,            CallingNameMapIp2Tel_SourcePrefix,            CallingNameMapIp2Tel_CallingNamePrefix,            CallingNameMapIp2Tel_SourceAddress,            CallingNameMapIp2Tel_RemoveFromLeft,            CallingNameMapIp2Tel_RemoveFromRight,            CallingNameMapIp2Tel_LeaveFromRight,            CallingNameMapIp2Tel_Prefix2Add,            CallingNameMapIp2Tel_Suffix2Add;  <b>[ \CallingNameMapIp2Tel ]</b></p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring SIP Calling Name Manipulation' on page <a href="#">304</a>.</p>
<b>Calling Name Manipulations Tel-to-IP Table</b>	
CLI: configure voip > gw manipulations calling-name-map-tel2ip <b>[CallingNameMapTel2Ip]</b>	<p>This table parameter configures rules for manipulating the calling name (caller ID) for Tel-to-IP calls. This can include modifying or removing the calling name.</p> <p><b>[ CallingNameMapTel2Ip ]</b></p>

Parameter	Description
	<p>FORMAT CallingNameMapTel2Ip_Index =  CallingNameMapTel2Ip_DestinationPrefix,  CallingNameMapTel2Ip_SourcePrefix,  CallingNameMapTel2Ip_CallingNamePrefix,  CallingNameMapTel2Ip_SrcTrunkGroupID,  CallingNameMapTel2Ip_SrcIPGroupID,  CallingNameMapTel2Ip_RemoveFromLeft,  CallingNameMapTel2Ip_RemoveFromRight,  CallingNameMapTel2Ip_LeaveFromRight,  CallingNameMapTel2Ip_Prefix2Add,  CallingNameMapTel2Ip_Suffix2Add;  [ \CallingNameMapTel2Ip ]</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring SIP Calling Name Manipulation' on page <a href="#">304</a>.</p>
<b>Destination Phone Number Manipulation for IP-to-Tel Calls Table</b>	
<p>Web: Destination Phone Number Manipulation Table for IP &gt; Tel Calls  EMS: SIP Manipulations &gt; Destination IP to Telcom  CLI: configure voip &gt; gw manipulations  NumberMapIp2Tel2  <b>[NumberMapIP2Tel]</b></p>	<p>This table parameter manipulates the destination number of IP-to-Tel calls. The format of this parameter is as follows:</p> <p><b>[NumberMapIp2Tel]</b>  FORMAT NumberMapIp2Tel_Index =  NumberMapIp2Tel_DestinationPrefix, NumberMapIp2Tel_SourcePrefix,  NumberMapIp2Tel_SourceAddress, NumberMapIp2Tel_NumberType,  NumberMapIp2Tel_NumberPlan, NumberMapIp2Tel_RemoveFromLeft,  NumberMapIp2Tel_RemoveFromRight,  NumberMapIp2Tel_LeaveFromRight, NumberMapIp2Tel_Prefix2Add,  NumberMapIp2Tel_Suffix2Add,  NumberMapIp2Tel_IsPresentationRestricted;  <b>[NumberMapIp2Tel]</b></p> <p>For example:  NumberMapIp2Tel 0 = 01,034,10.13.77.8,\$\$,0,\$\$,2,\$\$,667,\$\$;  NumberMapIp2Tel 1 = 10,10,1.1.1.1,255,255,3,0,5,100,\$\$,255;</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring Source/Destination Number Manipulation' on page <a href="#">297</a>.</p>
<p>EMS: Perform Additional IP2TEL Destination Manipulation  CLI: prfm-ip-to-tel-dst-map  <b>[PerformAdditionalIP2TEL DestinationManipulation]</b></p>	<p>Enables additional destination number manipulation for IP-to-Tel calls. The additional manipulation is done on the initially manipulated destination number, and this additional rule is also configured in the manipulation table (NumberMapIP2Tel parameter). This enables you to configure only a few manipulation rules for complex number manipulation requirements (that generally require many rules).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul>
<b>Destination Phone Number Manipulation for Tel-to-IP Calls Table</b>	
<p>Web: Destination Phone Number Manipulation Table for Tel &gt; IP Calls  EMS: SIP Manipulations &gt; Destination Telcom to IPs  CLI: configure voip &gt; gw manipulations  NumberMapTel2Ip  <b>[NumberMapTel2IP]</b></p>	<p>This table parameter manipulates the destination number of Tel-to-IP calls. The format of this parameter is as follows:</p> <p><b>[NumberMapTel2Ip]</b>  FORMAT NumberMapTel2Ip_Index =  NumberMapTel2Ip_DestinationPrefix, NumberMapTel2Ip_SourcePrefix,  NumberMapTel2Ip_SourceAddress, NumberMapTel2Ip_NumberType,  NumberMapTel2Ip_NumberPlan, NumberMapTel2Ip_RemoveFromLeft,  NumberMapTel2Ip_RemoveFromRight,  NumberMapTel2Ip_LeaveFromRight, NumberMapTel2Ip_Prefix2Add,  NumberMapTel2Ip_Suffix2Add,  NumberMapTel2Ip_IsPresentationRestricted,  NumberMapTel2Ip_SrcTrunkGroupID, NumberMapTel2Ip_</p>



Parameter	Description
	<p>SrcIPGroupID;  <b>[NumberMapTel2Ip]</b></p> <p>For example:  NumberMapTel2Ip 0 = 01,\$\$,*,0,0,2,\$\$,971,\$\$,,\$\$,,\$\$;  NumberMapTel2Ip 1 = 10,10,*,255,255,3,0,5,100,\$\$,255,\$\$,,\$\$;</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring Source/Destination Number Manipulation' on page 297.</p>
<b>Source Phone Number Manipulation for IP-to-Tel Calls Table</b>	
<p>Web: Source Phone Number Manipulation Table for IP &gt; Tel Calls  EMS: SIP Manipulations &gt; Source IP to Telcom  CLI: configure voip &gt; gw manipulations  SourceNumberMapIp2Tel  <b>[SourceNumberMapIP2Tel]</b></p>	<p>This <i>parameter</i> table manipulates the source number for IP-to-Tel calls. The format of this parameter is as follows:  <b>[SourceNumberMapIp2Tel]</b>  FORMAT SourceNumberMapIp2Tel_Index = SourceNumberMapIp2Tel_DestinationPrefix, SourceNumberMapIp2Tel_SourcePrefix, SourceNumberMapIp2Tel_SourceAddress, SourceNumberMapIp2Tel_NumberType, SourceNumberMapIp2Tel_NumberPlan, SourceNumberMapIp2Tel_RemoveFromLeft, SourceNumberMapIp2Tel_RemoveFromRight, SourceNumberMapIp2Tel_LeaveFromRight, SourceNumberMapIp2Tel_Prefix2Add, SourceNumberMapIp2Tel_Suffix2Add, SourceNumberMapIp2Tel_IsPresentationRestricted;  <b>[SourceNumberMapIp2Tel]</b></p> <p>For example:  SourceNumberMapIp2Tel 0 = 22,03,\$\$,,\$\$,,\$\$,2,667,\$\$,,\$\$;  SourceNumberMapIp2Tel 1 = 034,01,1.1.1.1,\$\$,0,2,\$\$,,\$\$,972,\$\$,10;</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring Source/Destination Number Manipulation' on page 297.</p>
<p>EMS: Perform Additional IP2TEL Source Manipulation  CLI: prfm-ip-to-tel-src-map  <b>[PerformAdditionalIP2TEL SourceManipulation]</b></p>	<p>Enables additional source number manipulation for IP-to-Tel calls. The additional manipulation is done on the initially manipulated source number, and this additional rule is also configured in the manipulation table (SourceNumberMapIP2Tel parameter). This enables you to configure only a few manipulation rules for complex number manipulation requirements (that generally require many rules).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul>
<b>Source Phone Number Manipulation for Tel-to-IP Calls Table</b>	
<p>Web: Source Phone Number Manipulation Table for Tel &gt; IP Calls  EMS: SIP Manipulations &gt; Source Telcom to IP  CLI: configure voip &gt; gw manipulations  SourceNumberMapTel2Ip  <b>[SourceNumberMapTel2IP]</b></p>	<p>This table parameter manipulates the source phone number for Tel-to-IP calls. The format of this parameter is as follows:  <b>[SourceNumberMapTel2Ip]</b>  FORMAT SourceNumberMapTel2Ip_Index = SourceNumberMapTel2Ip_DestinationPrefix, SourceNumberMapTel2Ip_SourcePrefix, SourceNumberMapTel2Ip_SourceAddress, SourceNumberMapTel2Ip_NumberType, SourceNumberMapTel2Ip_NumberPlan, SourceNumberMapTel2Ip_RemoveFromLeft, SourceNumberMapTel2Ip_RemoveFromRight, SourceNumberMapTel2Ip_LeaveFromRight, SourceNumberMapTel2Ip_Prefix2Add,</p>

Parameter	Description
	<p>SourceNumberMapTel2Ip_Suffix2Add, SourceNumberMapTel2Ip_IsPresentationRestricted, NumberMapTel2Ip_SrcTrunkGroupID, NumberMapTel2Ip_SrcIPGroupID; <b>[SourceNumberMapTel2Ip]</b></p> <p>For example: SourceNumberMapTel2Ip 0 = 22,03,\$\$,0,0,\$\$,2,\$\$,667,\$\$,0,\$\$,,\$\$; SourceNumberMapTel2Ip 0 = 10,10,* ,255,255,3,0,5,100,\$\$,255,\$\$,,\$\$;</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring Source/Destination Number Manipulation' on page 297.</p>
<b>Redirect Number IP -to-Tel Table</b>	
<p>Web: Redirect Number IP -&gt; Tel EMS: Redirect Number Map IP to Tel CLI: configure voip &gt; gw manipulations redirect-number-map-ip2tel <b>[RedirectNumberMapIp2Tel]</b></p>	<p>This table parameter manipulates the redirect number for IP-to-Tel calls. The format of this parameter is as follows: <b>[RedirectNumberMapIp2Tel]</b> FORMAT RedirectNumberMapIp2Tel_Index = RedirectNumberMapIp2Tel_DestinationPrefix, RedirectNumberMapIp2Tel_RedirectPrefix, RedirectNumberMapIp2Tel_SourceAddress, RedirectNumberMapIp2Tel_SrcHost, RedirectNumberMapIp2Tel_DestHost, RedirectNumberMapIp2Tel_NumberType, RedirectNumberMapIp2Tel_NumberPlan, RedirectNumberMapIp2Tel_RemoveFromLeft, RedirectNumberMapIp2Tel_RemoveFromRight, RedirectNumberMapIp2Tel_LeaveFromRight, RedirectNumberMapIp2Tel_Prefix2Add, RedirectNumberMapIp2Tel_Suffix2Add, RedirectNumberMapIp2Tel_IsPresentationRestricted; <b>[RedirectNumberMapIp2Tel]</b></p> <p>For example: RedirectNumberMapIp2Tel 1 = *, 88, *, , , 1, 1, 2, 0, 255, 9, , 255;</p> <p><b>Note:</b> For a description of this table, see Configuring Redirect Number Manipulation on page 307.</p>
<b>Redirect Number Tel-to-IP Table</b>	
<p>Web: Redirect Number Tel -&gt; IP EMS: Redirect Number Map Tel to IP CLI: configure voip &gt; gw manipulations redirect-number-map-tel2ip <b>[RedirectNumberMapTel2IP]</b></p>	<p>This table parameter manipulates the Redirect Number for Tel-to-IP calls. The format of this parameter is as follows: <b>[RedirectNumberMapTel2Ip]</b> FORMAT RedirectNumberMapTel2Ip_Index = RedirectNumberMapTel2Ip_DestinationPrefix, RedirectNumberMapTel2Ip_RedirectPrefix, RedirectNumberMapTel2Ip_RemoveFromLeft, RedirectNumberMapTel2Ip_RemoveFromRight, RedirectNumberMapTel2Ip_LeaveFromRight, RedirectNumberMapTel2Ip_Prefix2Add, RedirectNumberMapTel2Ip_Suffix2Add, RedirectNumberMapTel2Ip_IsPresentationRestricted, RedirectNumberMapTel2Ip_SrcTrunkGroupID, RedirectNumberMapTel2Ip_SrcIPGroupID; <b>[RedirectNumberMapTel2Ip]</b></p> <p>For example: RedirectNumberMapTel2Ip 1 = *, *, 4, 0, 255, , , 255, -1, -1;</p> <p><b>Note:</b> For a description of this table, see 'Configuring Redirect Number Manipulation' on page 307.</p>



Parameter	Description
<b>Phone Context Table</b>	
Web: Phone Context Table EMS: SIP Manipulations > Phone Context CLI: configure voip > gw manipulations phone-context-table <b>[PhoneContext]</b>	This table parameter configures the Phone Context table. This parameter maps NPI and TON to the SIP 'phone-context' parameter, and vice versa.  The format for this parameter is as follows: <b>[PhoneContext]</b> FORMAT PhoneContext_Index = PhoneContext_Npi, PhoneContext_Ton, PhoneContext_Context; <b>[PhoneContext]</b>  For example: PhoneContext 0 = 0,0,unknown.com PhoneContext 1 = 1,1,host.com PhoneContext 2 = 9,1,na.e164.host.com  <b>Note:</b> For a detailed description of this table, see 'Mapping NPI/TON to SIP Phone-Context' on page 311.
Web/EMS: Add Phone Context As Prefix CLI: add-ph-cntxt-as-pref <b>[AddPhoneContextAsPrefix]</b>	Determines whether the received Phone-Context parameter is added as a prefix to the outgoing ISDN Setup message with (for digital interfaces) Called and Calling numbers. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>

## 59.12 Least Cost Routing Parameters

The Least Cost Routing (LCR) parameters are described in the table below.

### LCR Parameters

Parameter	Description
Web: Routing Rule Groups Table CLI: configure voip > services least-cost-routing routing-rule-groups <b>[RoutingRuleGroups]</b>	This table parameter enables the LCR feature and configures the average call duration and default call cost. The default call cost determines whether routing rules that are not configured with a Cost Group are considered as a higher or lower cost route compared to other matching routing rules that are assigned Cost Groups.  <b>[ RoutingRuleGroups ]</b> FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable, RoutingRuleGroups_LCRAverageCallLength, RoutingRuleGroups_LCRDefaultCost; <b>[ \RoutingRuleGroups ]</b>  <b>Note:</b> For a detailed description of this table, see 'Enabling LCR and Configuring Default LCR' on page 191.
Web: Cost Group Table EMS: Cost Group Provisioning > Cost Group CLI: configure voip > services least-cost-routing cost-group <b>[CostGroupTable]</b>	This table parameter configures the Cost Groups for LCR, where each Cost Group is configured with a name, fixed call connection charge, and a call rate (charge per minute).  <b>[ CostGroupTable ]</b> FORMAT CostGroupTable_Index = CostGroupTable_CostGroupName, CostGroupTable_DefaultConnectionCost, CostGroupTable_DefaultMinuteCost; <b>[ \CostGroupTable ]</b>

Parameter	Description
	For example: CostGroupTable 2 = "Local Calls", 2, 1; <b>Note:</b> For a detailed description of this table, see 'Configuring Cost Groups' on page 193.
Web: Cost Group > Time Band Table EMS: Time Band Provisioning > Time Band CLI: configure voip > services least-cost-routing cost-group-time-bands <b>[CostGroupTimebands]</b>	This table parameter configures time bands and associates them with Cost Groups. <b>[CostGroupTimebands]</b> FORMAT CostGroupTimebands_TimebandIndex = CostGroupTimebands_StartTime, CostGroupTimebands_EndTime, CostGroupTimebands_ConnectionCost, CostGroupTimebands_MinuteCost; <b>[CostGroupTimebands]</b> <b>Note:</b> For a detailed description of this table, see 'Configuring Time Bands for Cost Groups' on page 194.

## 59.13 LDAP Parameters

The Lightweight Directory Access Protocol (LDAP) parameters are described in the table below. For more information on routing based on LDAP, see 'Routing Based on LDAP Active Directory Queries' on page 179.

**LDAP Parameters**

Parameter	Description
Web: LDAP Service CLI: enable <b>[LDAPServiceEnable]</b>	Enables the LDAP feature. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: LDAP Server IP EMS: Server Ip <b>[LDAPServerIP]</b>	Defines the LDAP server's address as an IP address (in dotted-decimal notation, e.g., 192.10.1.255). The default is 0.0.0.0.
Web: LDAP Server Port EMS: Server Port CLI: server-port <b>[LDAPServerPort]</b>	Defines the LDAP server's port number. The valid value range is 0 to 65535. The default port number is 389.
Web: LDAP Server Domain Name EMS: Server Domain Name CLI: server-domain-name <b>[LDAPServerDomainName]</b>	Defines the host name (FQDN) of the LDAP server. The device tries to connect to the LDAP server according to the IP address list received in the DNS query. If there is no connection to the LDAP server or the connection to the LDAP server fails, the device tries to connect to the LDAP server with the next IP address in the DNS query list. <b>Note:</b> The 'LDAP Server IP' parameter takes precedence over this parameter. Thus, if you want to use an FQDN, keep the 'LDAP Server IP' parameter empty.
Web: LDAP Password EMS: Password <b>[LDAPPassword]</b>	Defines the LDAP server's user password.
Web: LDAP Bind DN EMS: Bind DN CLI: password	Defines the LDAP server's bind Distinguished Name (DN). This is used as the username during connection and binding to the server. For example: LDAPBindDN = "CN=Search

Parameter	Description
<b>[LDAPBindDN]</b>	<p>user,OU=Labs,DC=OCSR2,DC=local"</p> <p><b>Note:</b> The DN is used to uniquely name an Active Directory object.</p>
Web: LDAP Search Dn EMS: Search DN CLI: search-dns <b>[LDAPSearchDN]</b>	<p>Defines up to three search DN's for LDAP search queries. These are the DN subtrees where the search is done. This parameter is mandatory for the search.</p> <p>The format of this parameter is as follows:</p> <p><b>[LdapSearchDNs ]</b>            FORMAT LdapSearchDNs_Index = LdapSearchDNs_Base_Path;  <b>[ \LdapSearchDNs ]</b></p> <p>For example:            LdapSearchDNs 0 = "CN=Search            user,OU=NY,DC=OCSR2,DC=local";            LdapSearchDNs 1 = "CN=Search            user,OU=SF,DC=OCSR2,DC=local";</p> <p>In this example, the DN path is defined by the LDAP names, cn (common name), ou (organizational unit) and dc (domain component).</p> <p><b>Note:</b> If you configure multiple DN's, you can specify whether the search is done sequentially or in parallel, using the LDAPSearchDNsinParallel parameter.</p>
CLI: search-dns-in-parallel <b>[LDAPSearchDNsinParallel]</b>	<p>Defines the LDAP query DN search method in the AD database if multiple search DN's are configured, using the LDAPSearchDNs parameter.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Sequential = If the first DN search fails, the search is done on the next configured DN, and so on.</li> <li><b>[1]</b> Parallel (Default)</li> </ul>
Web: LDAP Server Max Respond Time EMS: Server Max Respond Time CLI: server-max-respond-time <b>[LDAPServerMaxRespondTime]</b>	<p>Defines the time (in seconds) that the device waits for LDAP server responses.</p> <p>The valid value range is 0 to 86400. The default is 3000.</p>
<b>[LDAPDebugMode]</b>	<p>Determines whether to enable the LDAP task debug messages. This is used for providing debug information regarding LDAP tasks.</p> <p>The valid value range is 0 to 3. The default is 0.</p>
Web: MS LDAP OCS Number attribute name EMS: LDAP ocs Number Attribute Name CLI: ldap-ocs-nm-attr <b>[MSLDAPOCSNumAttribute Name]</b>	<p>Defines the name of the attribute that represents the user OCS number in the Microsoft AD database.</p> <p>The valid value is a string of up to 49 characters. The default is "msRTCSIP-PrimaryUserAddress".</p>
Web: MS LDAP PBX Number attribute name CLI: ldap-pbx-nm-attr <b>[MSLDAPPBXNumAttribute Name]</b>	<p>Defines the name of the attribute that represents the user PBX number in the Microsoft AD database.</p> <p>The valid value is a string of up to 49 characters. The default is "telephoneNumber".</p>

Parameter	Description
Web: MS LDAP MOBILE Number attribute name CLI: ldap-mobile-nm-attr <b>[MSLDAPMobileNumAttribute]</b>	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".
CLI: ldap-private-nm-attr <b>[MSLDAPPrivateNumAttribute]</b>	Defines the name of the attribute that represents the user's private number in the AD. If this value equals the value of the MSLDAPPrimaryKey or MSLDAPSecondaryKey parameter, then the device queries the AD for the destination number in this private attribute name; otherwise, this parameter is not used as a search key.  The default is "msRTCSIP-PrivateLine".
CLI: ldap-display-nm-attr <b>[MSLDAPDisplayNameAttribute]</b>	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".
CLI: ldap-primary-key <b>[MSLDAPPrimaryKey]</b>	Defines the name of the attribute used as a query search key for the destination number in the AD. This is used instead of the "PBX" attribute name (configured by the MSLDAPPBXNumAttributeName parameter).  The default is not configured.
CLI: ldap-secondary-key <b>[MSLDAPSecondaryKey]</b>	Defines the name of the attribute used as the second query search key for the destination number in the AD, if the primary search key or PBX search is not found.
LDAP Cache Service CLI: cache <b>[LDAPCacheEnable]</b>	Enables the LDAP cache service. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For more information on LDAP caching, see 'Configuring the Device's LDAP Cache' on page <a href="#">180</a>.</li> </ul>
LDAP Cache Entry Timeout CLI: entry-timeout <b>[LDAPCacheEntryTimeout]</b>	Defines the duration (in minutes) that an entry in the LDAP cache is valid. If the timeout expires, the cached entry is only used if there is no connectivity with the LDAP server.  The default is 1200.
LDAP Cache Entry Removal Timeout CLI: entry-removal-timeout <b>[LDAPCacheEntryRemovalTimeout]</b>	Defines the duration (in hours) after which the LDAP entry is removed from the cache.  The default is 0.

## 59.14 SBC and CRP Parameters

The SBC and CRP parameters are described in the table below.

**SBC and CRP Parameters**

Parameter	Description
<b>CRP-Specific Parameters</b>	
Web: CRP Application CLI: enable-crp <b>[EnableCRPApplication]</b>	<p>Enables the CRP application.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: CRP Survivability Mode CLI: crp-survivability-mode <b>[CRPSurvivabilityMode]</b>	<p>Defines the CRP mode.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Standard Mode (default)</li> <li>▪ <b>[1]</b> Always Emergency Mode</li> <li>▪ <b>[2]</b> Auto-answer REGISTER</li> </ul>
<b>SBC-Specific Parameters</b>	
Web/EMS: Enable SBC CLI: enable-sbc <b>[EnableSBCApplication]</b>	<p>Enables the Session Border Control (SBC) application.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ In addition to enabling this parameter, the number of maximum SBC/IP-to-IP sessions must be defined in the Software License Key.</li> </ul>
<b>SBC and CRP Parameters</b>	
WAN Interface Name <b>[WanInterfaceName]</b>	<p>Defines the WAN interface for the VoIP interface. The available interface options depends on the hardware configuration (e.g., Ethernet or SHDSL) and/or whether VLANs are defined for the WAN interface.</p> <p>The value must be enclosed in single quotation marks ('...'), for example, WanInterfaceName = 'GigabitEthernet 0/0'.</p> <p>This WAN interface can be assigned to SIP signaling and/or media interfaces, in the SIP Interface table, where it is represented as "WAN" (see Configuring SIP Interface Table on page 201). If VLANs are configured, for example, for the Ethernet WAN interface, then you can select the WAN VLAN on which you want to run these SIP signaling and/or media interfaces. Therefore, for each outgoing SIP packet, the device sends it on the defined outgoing WAN interface; for each incoming SIP packet, the device identifies the packet according to the WAN interface from where it is received.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ This parameter is applicable only if the data-routing functionality is supported (i.e., relevant Software License Key is installed on the device).</li> </ul>

Parameter	Description
Web: Allow Unclassified Calls CLI: unclassified-calls <b>[AllowUnclassifiedCalls]</b>	<p>Determines whether incoming calls that cannot be classified (i.e. classification process fails) to a Source IP Group are rejected or processed.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Reject = Call is rejected if classification fails.</li> <li>▪ <b>[1]</b> Allow = (Default) If classification fails, the incoming packet is assigned to a source IP Group (and subsequently processed) as follows: <ul style="list-style-type: none"> <li>✓ The source SRD is determined according to the SIP Interface to where the SIP-initiating dialog request is sent. The source IP Group is set to the default IP Group associated with this SRD.</li> <li>✓ If the source SRD is ID 0, then source IP Group ID 0 is chosen. In case of any other SRD, then the first IP Group associated with this SRD is chosen as the source IP Group or the call. If no IP Group is associated with this SRD, the call is rejected.</li> </ul> </li> </ul>
Web: SBC No Answer Timeout CLI: sbc-no-arelt-timeout <b>[SBCAlertTimeout]</b>	<p>Defines the timeout (in seconds) for SBC outgoing (outbound IP routing) SIP INVITE messages. If the called IP party does not answer the call within this user-defined interval, the device disconnects the session. The device starts the timeout count upon receipt of a SIP 180 Ringing response from the called party. If no other SIP response (for example, 200 OK) is received thereafter within this timeout, the call is released.</p> <p>The valid range is 0 to 3600 seconds. the default is 600.</p>
Web: SBC Max Forwards Limit CLI: sbc-max-fwd-limit <b>[SBCMaxForwardsLimit]</b>	<p>Defines the Max-Forwards SIP header value. The Max-Forwards header is used to limit the number of servers (such as proxies) that can forward the SIP request. The Max-Forwards value indicates the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request.</p> <p>This parameter affects the Max-Forwards header in the received message as follows:</p> <ul style="list-style-type: none"> <li>▪ If the received header's original value is 0, the message is not passed on and is rejected.</li> <li>▪ If the received header's original value is less than this parameter's value, the header's value is decremented before being sent on.</li> <li>▪ If the received header's original value is greater than the parameter's value, the header's value is replaced by the user-defined parameter's value.</li> </ul> <p>The valid value range is 1-70. The default is 10.</p>
Web: SBC Session-Expires CLI: sbc-sess-exp-time <b>[SBCSessionExpires]</b>	<p>Defines the SBC session refresh timer (in seconds) in the Session-Expires header of outgoing INVITE messages.</p> <p>The valid value range is 90 (according to RFC 4028) to 86400. The default is 180.</p>
Web: Minimum Session-Expires CLI: min-session-expires <b>[SBCMinSE]</b>	<p>Defines the minimum amount of time (in seconds) between session refresh requests in a dialog before the session is considered timed out. This value is conveyed in the SIP Min-SE header.</p> <p>The valid range is 0 (default) to 1,000,000 (where 0 means that the device does not limit Session-Expires).</p>
Web/EMS: Handle P-Asserted-Identity	<p>Determines the device's privacy handling of the P-Asserted-Identity header. This indicates how the outgoing SIP message asserts</p>

Parameter	Description
CLI: p-assert-id <b>[SBCAssertIdentity]</b>	<p>identity.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Don't Care = (Default) P-Asserted Identity header is not affected.</li> <li>▪ <b>[1]</b> Add P-Asserted-Identity Header = Adds a P-Asserted-Identity header. The header's values are taken from the source URL.</li> <li>▪ <b>[2]</b> Remove P-Asserted-Identity Header = Removes the P-Asserted-Identity header.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter affects only the initial INVITE request.</li> <li>▪ The configuration of privacy handling in the IP Group table takes precedence over the settings of this global parameter.               <ul style="list-style-type: none"> <li>✓ If in the IP Group this parameter is set to 'Don't care', then the settings of this global parameter is used.</li> <li>✓ If this global parameter and the IP Group are set to 'Don't care', the device uses the same P-Asserted-Identity header (if present) in the incoming message for the outgoing message.</li> </ul> </li> <li>▪ This parameter can also be configured in an IP Profile.</li> </ul>
Web: Keep original user in Register <b>[SBCKeepContactUserinRegister]</b>	<p>Determines whether the device replaces the Contact user with a unique Contact user in the outgoing message in response to a REGISTER request.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) The device replaces the original Contact user with a unique Contact user, for example:               <ul style="list-style-type: none"> <li>✓ Received Contact: &lt;sip:123@domain.com&gt;</li> <li>✓ Outgoing (unique) Contact: &lt;sip:FEU1_7_1@SBC&gt;</li> </ul> </li> <li>▪ <b>[1]</b> Enable = The original Contact user is retained and used in the outgoing REGISTER request.</li> </ul> <p><b>Note:</b> This parameter is applicable only to REGISTER messages received from User-type IP Groups and that are sent to Server-type IP Groups.</p>
Web: SBC Remote Refer Behavior CLI: sbc-refer-bhvr <b>[SBCReferBehavior]</b>	<p>Determines the device's handling of REFER requests.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Transparent = (Default) Refer-To header is unchanged and the device forwards the REFER as is.</li> <li>▪ <b>[1]</b> DB URL = Changes the Refer-To header so that the re-routed INVITE is sent through the SBC:               <ol style="list-style-type: none"> <li>Before forwarding the REFER request, the device changes the host part to the device's IP address and adds a special prefix ("T~&amp;R_") to the Contact user part.</li> <li>The incoming INVITE is identified as a REFER-resultant INVITE according to this special prefix.</li> <li>The device replaces the host part in the Request-URI with the host from the REFER contact. The special prefix remains in the user part for regular classification, manipulation, and routing. The special prefix can also be used for specific routing rules for REFER-resultant INVITES.</li> <li>The special prefix is removed before the resultant INVITE is sent to the destination.</li> </ol> </li> <li>▪ <b>[2]</b> IP Group Name = Sets the host part in the REFER message to the name defined for the IP Group (in the IP Group table).</li> <li>▪ <b>[3]</b> 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</li> </ul>



Parameter	Description
	<p>IP-to-IP Routing table (the 'Call Trigger' field must be set to <b>REFER</b>).</p> <p><b>Note:</b> This parameter can be configured in an IP Profile.</p>
CLI: sbc-xfer-prefix <b>[SBCXferPrefix]</b>	<p>When the SBCReferBehavior is set to 1, the device, while interworking the SIP REFER message, adds the prefix "T~&amp;R-" to the user part of the URI in the Refer-To header. After this, the device can receive an INVITE with such a prefix (the INVITE is sent by the UA that receives the REFER message or 302 response). If the device receives an INVITE with such a prefix, it replaces the prefix with the value defined for the SBCXferPrefix parameter.</p> <p>The default value is empty ("").</p> <p><b>Note:</b> This feature is also applicable to 3xx redirect responses. The device adds the prefix "T~&amp;R-" to the URI user part in the Contact header if the SBC3xxBehavior parameter is set to 1.</p>
CLI: sbc-3xx-bhvt <b>[SBC3xxBehavior]</b>	<p>Determines the device's handling of SIP 3xx responses. When enabled, the device handles SIP redirections between different subnets (e.g., between LAN and WAN sides). This is required where the new address provided by the redirector (Redirect sever) may not be reachable by the far-end user (FEU) located in another subnet. For example, a far-end user (FEU) in the WAN sends a SIP request via the device to a Redirect server in the LAN, and the Redirect server replies with a SIP 3xx response to a PBX in the LAN in the Contact header. If the device sends this response as is (i.e., with the original Contact header), the FEU is unable to reach the new destination.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Transparent = (Default)</b> The device forwards the received SIP 3xx response as is, without changing the Contact header (i.e., transparent handling).</li> <li>▪ <b>[1] DB URL =</b> The device changes the Contact header so that the re-route request is sent through the the device. The device changes the URI in the Contact header of the received SIP 3xx response to its own URI and adds a special user prefix ("T~&amp;R_"), which is then sent to the FEU. The FEU then sends a new INVITE to the device, which the device then sends to the correct destination.</li> <li>▪ <b>[2] Handle Locally =</b> The device handles SIP 3xx responses on behalf of the dialog-initiating UA and retries the request (e.g., INVITE) using one or more alternative URIs included in the 3xx response. The device sends the new request to the alternative destination according to the IP-to-IP Routing table (the 'Call Trigger' field must be set to <b>3xx</b>).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ When this parameter is changed from 1 to 0, new 3xx Contact headers remain unchanged. However, requests with the special prefix continue using the device's database to locate the new destination.</li> <li>▪ Only one database entry is supported for the same host, port, and transport combination. For example, the following URLs cannot be distinguished by the device:               <ul style="list-style-type: none"> <li>✓ sip:10.10.10.10:5060;transport=tcp;param=a</li> <li>✓ sip:10.10.10.10:5060;transport=tcp;param=b</li> </ul> </li> <li>▪ The database entry expires two hours after the last use.</li> <li>▪ The maximum number of destinations (i.e., database entries) is</li> </ul>



Parameter	Description
	<p>50.</p> <ul style="list-style-type: none"> <li>This parameter can also be configured as an IP Profile.</li> <li>For more information on SIP 3xx Redirect response handling, see 'Handling SIP 3xx Redirect Responses' on page 436.</li> </ul>
Web: Enforce Media Order <b>[SBCEnforceMediaOrder]</b>	<p>Enables the device to arrange media lines ('m=' line) in the SDP offer according to the previous offer-answer exchange (RFC 3264).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul>
Web: Lifetime of the nonce in seconds CLI: lifetime-of-nonce <b>[AuthNonceDuration]</b>	<p>Defines the lifetime (in seconds) that the current nonce is valid for server-based authentication. The device challenges a message that attempts to use a server nonce beyond this period. This parameter is used to provide replay protection (i.e., ensures that old communication streams are not used in replay attacks).</p> <p>The valid value range is 30 to 600. The default is 300.</p>
Web: Authentication Challenge Method CLI: auth-chlng-mthd <b>[AuthChallengeMethod]</b>	<p>Defines the type of server-based authentication challenge.</p> <ul style="list-style-type: none"> <li><b>[0]</b> 0 = (Default) Send SIP 401 "Unauthorized" with a WWW-Authenticate header as the authentication challenge response.</li> <li><b>[1]</b> 1 = Send SIP 407 "Proxy Authentication Required" with a Proxy-Authenticate header as the authentication challenge response.</li> </ul>
Web: Authentication Quality of Protection CLI: auth-qop <b>[AuthQOP]</b>	<p>Defines the authentication and integrity level of quality of protection (QoP) for digest authentication offered to the client. When the device challenges a SIP request (e.g., INVITE), it sends a SIP 401 response with the Proxy-Authenticate header or WWW-Authenticate header containing the 'qop' parameter. The QoP offered in the 401 response can be 'auth', 'auth-int', both 'auth' and 'auth-int', or the 'qop' parameter can be omitted from the 401 response. In response to the 401, the client needs to send the device another INVITE with the MD5 hash of the INVITE message and indicate the selected auth type.</p> <ul style="list-style-type: none"> <li><b>[0]</b> 0 = The device sends 'qop=auth' in the SIP response, requesting authentication (i.e., validates user by checking user name and password). This option does not authenticate the message body (i.e., SDP).</li> <li><b>[1]</b> 1 = The device sends 'qop=auth-int' in the SIP response, indicating required authentication and authentication with integrity (e.g., checksum). This option restricts the client to authenticating the entire SIP message, including the body, if present.</li> <li><b>[2]</b> 2 = (Default) The device sends 'qop=auth, auth-int' in the SIP response, indicating either authentication or integrity. This enables the client to choose 'auth' or 'auth-int'. If the client chooses 'auth-int', then the body is included in the authentication. If the client chooses 'auth', then the body is not authenticated.</li> <li><b>[3]</b> 3 = No 'qop' parameter is offered by the device in the SIP 401 challenge message.</li> </ul>

Parameter	Description
Web: SBC User Registration Time CLI: sbc-usr-reg-time <b>[SBCUserRegistrationTime]</b>	<p>Defines the duration (in seconds) of the periodic registrations between the user and the device (the device responds with this value to the user). When set to 0, the device does not change the Expires header's value received in the user's REGISTER request. If no Expires header is received in the REGISTER message and the SBCUserRegistrationTime parameter is set to 0, then by default, the Expires header's value is set to 180 seconds.</p> <p>The valid range is 0 to 2,000,000 seconds. The default is 0.</p> <p><b>Note:</b> This parameter can also be configured for an IP Profile (in the IP Profile table).</p>
Web: SBC Proxy Registration Time CLI: sbc-prxy-reg-time <b>[SBCProxyRegistrationTime]</b>	<p>Defines the duration (in seconds) for which the user is registered in the proxy database (after the device forwards the REGISTER message). When set to 0, the device sends the Expires header's value as received from the user to the proxy.</p> <p>The valid range is 0 to 2,000,000 seconds. The default is 0.</p>
Web: SBC Survivability Registration Time CLI: sbc-surv-reg-time <b>[SBCSurvivabilityRegistrationTime]</b>	<p>Defines the duration of the periodic registrations between the user and the device, when the device is in survivability state (i.e., when REGISTER requests cannot be forwarded to the proxy and are terminated by the device). When set to 0, the device uses the value set by the SBCUserRegistrationTime parameter for the device's response.</p> <p>The valid range is 0 to 2,000,000 seconds. The default is 0.</p>
<b>[SBCEnableAASTRASurvivabilityNotice]</b>	<p>Enables the device to notify Aastra IP phones that the device is currently operating in Survivability mode. When this occurs, the Aastra IP phones display the message, "Stand Alone Mode" on their LCD screens. Survivability mode occurs when connectivity with the WAN fails and as a result, the device enables communication between IP phone users within the LAN enterprise.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable</li> <li>▪ <b>[1]</b> = Enable</li> </ul> <p>When this feature is enabled and the SBC device is in Survivability mode, it responds to SIP REGISTER messages from the IP phones with a SIP 200 OK containing the following XML body:</p> <pre>Content-Type: application/xml &lt;?xml version="1.0" encoding="utf-8"?&gt; &lt;LMIDocument version="1.0"&gt;   &lt;LocalModeStatus&gt;     &lt;LocalModeActive&gt;true&lt;/LocalModeActive&gt;     &lt;LocalModeDisplay&gt;StandAlone Mode&lt;/LocalModeDisplay&gt;   &lt;/LocalModeStatus&gt; &lt;/LMIDocument&gt;</pre>
Web: SBC GRUU Mode CLI: sbc-gruu-mode <b>[SBCGruuMode]</b>	<p>Determines the Globally Routable User Agent (UA) URI (GRUU) support, according to RFC 5627.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> None = No GRUU is supplied to users.</li> <li>▪ <b>[1]</b> As Proxy = (Default) The device provides same GRUU types as the proxy provided the device's GRUU clients.</li> <li>▪ <b>[2]</b> Temporary only = Supply only temporary GRUU to users. (Currently not supported.)</li> <li>▪ <b>[3]</b> Public only = The device provides only public GRUU to users.</li> <li>▪ <b>[4]</b> Both = The device provides temporary and public GRUU to</li> </ul>

Parameter	Description
	<p>users. (Currently not supported.)</p> <p>This parameter allows the device to act as a GRUU server for its SIP UA clients, providing them with public GRUU's, according to RFC 5627. The public GRUU provided to the client is denoted in the SIP Contact header parameters, "pub-gruu". Public GRUU remains the same over registration expirations. On the other SBC leg communicating with the Proxy/Registrar, the device acts as a GRUU client.</p> <p>The device creates a GRUU value for each of its registered clients, which is mapped to the GRUU value received from the Proxy server. In other words, the created GRUU value is only used between the device and its clients (endpoints).</p> <p>Public-GRUU: sip:userA@domain.com;gr=unique-id</p>
Web: Bye Authentication CLI: sbc-bye-auth <b>[SBCEnableByeAuthentication]</b>	<p>Enables authenticating a SIP BYE request before disconnecting the call. This feature prevents, for example, a scenario in which the SBC SIP client receives a BYE request from a third-party imposer assuming the identity of a participant in the call and as a consequence, the call between the first and second parties is inappropriately disconnected.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable = The device forwards the SIP authentication response (for the BYE request) to the request sender and waits for the user to authenticate it. The call is disconnected only if the authenticating server responds with a 200 OK.</li> </ul>
<b>[SBCExtensionsProvisioningMode]</b>	<p>Enables SBC user registration for interoperability with BroadSoft's BroadWorks server, to provide call survivability in case of connectivity failure with the BroadWorks server.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Normal processing of REGISTER messages.</li> <li>▪ <b>[1]</b> = Registration method for BroadWorks server. In a failure scenario with BroadWorks, the device acts as a backup SIP proxy server, maintaining call continuity between the enterprise LAN users (subscribers) and between the subscribers and the PSTN (if provided).</li> </ul> <p><b>Note:</b> For a detailed description of this feature, see 'Auto-Provisioning of Subscriber-Specific Information for BroadWorks Server' on page 443.</p>
Web: SBC Direct Media CLI: sbc-direct-media <b>[SBCDirectMedia]</b>	<p>Enables the No Media Anchoring feature (i.e., direct media) for all SBC calls. No Media Anchoring uses SIP signaling capabilities without handling the RTP/SRTP (media) flow between remote SIP user agents (UA). The RTP packets do not traverse the device, instead, the two SIP UAs establish a direct RTP/SRTP flow between one another. Signaling continues to traverse the device with minimal intermediation and involvement to enable certain SBC abilities such as routing</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) All SRD calls via SBC are not direct media - internal SRD calls are according to SRD configuration.</li> <li>▪ <b>[1]</b> Enable = All SBC calls use the No Media Anchoring feature (i.e., direct media).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For more information on No Media Anchoring, see 'No Media Anchoring (Anti Tromboning)' on page 429.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>When No Media Anchoring is enabled: <ul style="list-style-type: none"> <li>✓ Manipulation is not done on SDP data (offer/answer transaction) such as ports and IP addresses.</li> <li>✓ Opening voice channels and allocation of IP media ports are not required.</li> <li>✓ Forced Transcoding and Extension Coders features are disabled for No Media Anchoring calls.</li> <li>✓ The Coder Restriction feature (Allowed Coders List) operates simultaneously with No Media Anchoring calls. Restricted coders are removed from the SDP offer message.</li> </ul> </li> <li>No Media Anchoring is typically implemented in the following scenarios: <ul style="list-style-type: none"> <li>✓ SBC device is located in the LAN.</li> <li>✓ Calls between two SIP UAs in the same LAN and signals are sent to a SIP proxy server that is located in the WAN.</li> <li>✓ SBC device does not do NAT traversal (for media) and all the users are in the same domain.</li> </ul> </li> <li>The benefits of implementing the No Media Anchoring feature includes the following: saves network bandwidth, reduces CPU usage (no RTP/SRTP handling), and avoids interference in SDP negotiation and header manipulation on RTP/SRTP.</li> <li>The process for handling the No Media Anchoring feature is as follows: <ul style="list-style-type: none"> <li>✓ Identifying a No Media Anchoring call according to configuration and the call's properties (such as source, destination, IP Group, and SRD).</li> <li>✓ Handling the identified No Media Anchoring call.</li> </ul> </li> <li>You can enable No Media Anchoring per SRD (using the IntraSRDMediaAnchoring parameter), whereby calls between two UAs that pertain to the same SRD (source and destination) are handled as a No Media Anchoring (direct media) call.</li> <li>Chosen configuration can't handle call from any UA to a foreign UA (vice versa) but both UAs belong to the same SRD and the parameter IntraSRDMediaAnchoring for that specific SRD is &gt; 0.</li> <li>When this parameter is disabled, No Media Anchoring calls between two UAs that belong to separate SRDs cannot be configured. No Media Anchoring calls between two UAs that belong to the same SRD is configurable only (in this case).</li> </ul>
Web: Transcoding Mode CLI: transcoding-mode <b>[TranscodingMode]</b>	<p>Defines the voice transcoding mode (media negotiation) between the two SBC legs for the SBC application.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Only if Required = (Default) Do not force transcoding. Many of the media settings (such as gain control) are not implemented on the voice stream. The SBC application passes packets RTP to RTP without any processing.</li> <li><b>[1]</b> Force = Forces transcoding on the outgoing SBC leg. The device's SBC application interworks the media by implementing DSP transcoding.</li> </ul> <p><b>Note:</b> This parameter can also be configured in an IP Profile.</p>
Web: SBC Preferences Mode <b>[SBCPreferencesMode]</b>	<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 (defined in the Allowed Coders Group table) in the outgoing SIP message (in the SDP).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Doesn't Include Extensions = (Default) Extension coders are</li> </ul>

Parameter	Description
	<p>added at the end of the coder list.</p> <ul style="list-style-type: none"> <li>[1] Include Extensions = Extension coders and Allowed coders are arranged according to their order of appearance in the Allowed Coders Group table.</li> </ul> <p><b>Note:</b> If the SBCExtensionCodersGroupID parameter of the IP Profile table is set to None, then this parameter is not applicable.</p>
<p>Web: SBC Send Invite To All Contacts</p> <p>CLI: sbc-send-invite-to-all-contacts</p> <p><b>[SBCSendInviteToAllContacts]</b></p>	<p>Enables call forking of INVITE message received with a Request-URI for a specific contact registered in the device's database, to all users under the same AOR as the contact.</p> <ul style="list-style-type: none"> <li>[0] Disable (default) = Sends the INVITE only to the contact of the received Request-URI.</li> <li>[1] Enable</li> </ul> <p><b>Note:</b> To configure call forking initiated by the device, see Initiating SIP Call Forking.</p>
<p>Web: SBC Shared Line Registration Mode</p> <p>CLI: sbc-shared-line-reg-mode</p> <p><b>[SBCSharedLineRegMode]</b></p>	<p>Enables the termination on the device of SIP REGISTER messages from secondary lines pertaining to the Shared Line feature.</p> <ul style="list-style-type: none"> <li>[0] Disable = (Default) Device forwards the REGISTER messages as is (i.e., not terminated on the device).</li> <li>[1] Enable = REGISTER messages of secondary lines are terminated on the device.</li> </ul> <p><b>Note:</b> The device always forwards REGISTER messages of the primary line.</p>
<p>Web: SBC Forking Handling Mode</p> <p>CLI: sbc-forking-handling-mode</p> <p><b>[SBCForkingHandlingMode]</b></p>	<p>Defines the handling of SIP 18x responses received due to call forking of an INVITE.</p> <ul style="list-style-type: none"> <li>[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 responds according to the PlayRBTone2TEL parameter and disregards the subsequent forking 18x responses.</li> <li>[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.</li> </ul>
<p>CLI: sbc-media-sync</p> <p><b>[EnableSBCMediaSync]</b></p>	<p>Enables SBC media synchronization process for calls established from SIP forking that is initiated by external proxy servers. It is possible that a call is established with the media not synchronized between the SBC legs. Media synchronization resolves this issue.</p> <ul style="list-style-type: none"> <li>[0] Disable</li> <li>[1] Enable (default)</li> </ul>
<b>Admission Control Table</b>	
<p>Web: Admission Control</p> <p>EMS: Call Admission Control</p> <p>CLI: configure voip &gt; sbc sbc-admission-control</p> <p><b>[SBCAdmissionControl]</b></p>	<p>This table parameter defines limitations on the number of allowed concurrent calls (SIP dialogs). This is useful for controlling bandwidth utilization between Voice and Data traffic.</p> <p>The format of this parameter is as follows:</p> <p><b>[SBCAdmissionControl]</b></p> <p>FORMAT SBCAdmissionControl_Index = SBCAdmissionControl_LimitType, SBCAdmissionControl_IPGroupID, SBCAdmissionControl_SRIDID,</p>

Parameter	Description
	<p>SBCAdmissionControl_RequestType, SBCAdmissionControl_RequestDirection, SBCAdmissionControl_Limit, SBCAdmissionControl_LimitPerUser, SBCAdmissionControl_Rate, SBCAdmissionControl_MaxBurst; <b>[SBCAdmissionControl]</b></p> <p>For example, the below configuration allows a maximum of 10 concurrent SIP INVITEs for IP Group 1: SBCAdmissionControl 1 = 0, 1, -1, 1, 0, 10, -1, 0, 0;</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring Admission Control' on page <a href="#">452</a>.</p>
<b>Allowed Audio Coders Table</b>	
<p>Web: Allowed Audio Coders CLI: configure voip &gt; sbc allowed-coders-group AllowedCodersGroup0 <b>[AllowedCodersGroup0]</b> <b>[AllowedCodersGroup1]</b> <b>[AllowedCodersGroup2]</b> <b>[AllowedCodersGroup3]</b> <b>[AllowedCodersGroup4]</b></p>	<p>This table parameter configures Allowed Coders Groups, which determines the coders that can be used for a specific SBC leg. Coders excluded from the Allowed Coders Group are removed from the SDP offer (only coders common between SDP offered coders and Allowed Coders are used). In addition, coders defined in top entries in the Allowed Coders Group are assigned higher priority than those entered in lower entries.</p> <p><b>[AllowedCodersGroupx]</b> FORMAT AllowedCodersGroup_Index = AllowedCodersGroup_Name; <b>[AllowedCodersGroup]</b></p> <p>For example, below represents two configured Allowed Coders Groups. Group 0 has two coders; Group 1 has one coder. The highest priority coder is G.723.1.</p> <p><b>[ AllowedCodersGroup0 ]</b> FORMAT AllowedCodersGroup0_Index = AllowedCodersGroup0_Name; AllowedCodersGroup0 0 = g7231; AllowedCodersGroup0 1 = g711Alaw64k; <b>[ \AllowedCodersGroup0 ]</b></p> <p><b>[ AllowedCodersGroup1 ]</b> FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup0_Name; AllowedCodersGroup1 0 = g711Ulaw64k; <b>[ \AllowedCodersGroup1 ]</b></p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring Allowed Coder Groups' on page <a href="#">454</a>.</p>
<b>Classification Table</b>	
<p>Web: Classification Table EMS: SBC Classification CLI: configure voip &gt; sbc routing classification <b>[Classification]</b></p>	<p>This table parameter configures the Classification table. This table classifies incoming SIP dialogs to Source IP Groups. The format of this parameter is as follows:</p> <p><b>[ Classification ]</b> FORMAT Classification_Index = Classification_MessageCondition, Classification_SrcSRDID, Classification_SrcAddress, Classification_SrcPort, Classification_SrcTransportType, Classification_SrcUsernamePrefix, Classification_SrcHost, Classification_DestUsernamePrefix, Classification_DestHost, Classification_ActionType, Classification_SrcIPGroupID; <b>[ \Classification ]</b></p> <p>For example: Classification 1 = 1, , 10.8.6.15, 5060, 2, *, *, *, *, 1, 4;</p>



Parameter	Description
	<b>Note:</b> For a detailed description of this table, see 'Configuring Classification Rules' on page <a href="#">456</a> .
<b>Condition Table</b>	
Web: Condition Table CLI: configure voip > sbc routing condition-table <b>[ConditionTable]</b>	This table parameter configures Condition rules for SIP messages using the same syntax as used in the SIP Message Manipulation table. These Condition rules are later assigned to Classification rules in the Classification table for enhancing the process of classifying incoming SIP dialogs to an IP Groups. <b>[ ConditionTable ]</b> FORMAT ConditionTable_Index = ConditionTable_Condition, ConditionTable_Description; <b>[ \ConditionTable ]</b> <b>Note:</b> For a detailed description of this table, see 'Configuring Condition Rules' on page <a href="#">461</a> .
<b>SBC IP-to-IP Routing Table</b>	
Web: IP-to-IP Routing Table EMS: IP to IP Routing CLI: configure voip > sbc routing ip2ip-routing <b>[IP2IPRouting]</b>	This table parameter configures the SBC IP-to-IP Routing table for routing incoming SIP messages such as INVITE messages to an IP destination. The format of this parameter is as follows: <b>[IP2IPRouting]</b> FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_RequestType, IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID, IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort, IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions, IP2IPRouting_CostGroup; <b>[ \IP2IPRouting ]</b> For example: IP2IPRouting 1 = -1, *, *, *, *, 0, , -1, 0, 0, 1, , , 0, -1, 0,; <b>Note:</b> For a detailed description of this table, see 'Configuring SBC IP-to-IP Routing' on page <a href="#">462</a> .
<b>SBC Alternative Routing Reasons Table</b>	
Web: SBC Alternative Routing Reasons EMS: Alternative Routing Reasons CLI: configure voip > sbc routing sbc-alternative-routing-reasons <b>[SBCAlternativeRoutingReasons]</b>	This table parameter configures the SBC Alternative Routing Reasons table. This table is used for alternative IP-to-IP routing. If 4xx, 5xx, or 6xx SIP responses are received as a result of outgoing SIP dialog-initiating methods (e.g., INVITE, OPTIONS, and SUBSCRIBE messages), the device re-sends the messages to an alternative route if the response is defined in this table and if there are alternative routes configured in the IP-to-IP Routing table. The format of this parameter is as follows: <b>[ SBCAlternativeRoutingReasons ]</b> FORMAT SBCAlternativeRoutingReasons_Index = SBCAlternativeRoutingReasons_ReleaseCause; <b>[ \SBCAlternativeRoutingReasons ]</b> For example: SBCAlternativeRoutingReasons 0 = 403; SBCAlternativeRoutingReasons 1 = 404; <b>Note:</b> For a detailed description of this table, see 'Configuring

Parameter	Description
	Alternative Routing Reasons' on page <a href="#">468</a> .
<b>IP to IP Inbound Manipulation Table</b>	
Web: IP to IP Inbound Manipulation EMS: IP to IP Inbound Manipulation CLI: configure voip > sbc manipulations ip-inbound-manipulation <b>[IPInboundManipulation]</b>	<p>This table parameter configures the IP to IP Inbound Manipulation table. This table allows you to manipulate the SIP URI user part (source and/or destination) of the inbound SIP dialog message. The format of this parameter is as follows:</p> <p><b>[IPInboundManipulation]</b>  FORMAT IPInboundManipulation_Index =  IPInboundManipulation_IsAdditionalManipulation,  IPInboundManipulation_ManipulatedURI,  IPInboundManipulation_ManipulationPurpose,  IPInboundManipulation_SrcIPGroupID,  IPInboundManipulation_SrcUsernamePrefix,  IPInboundManipulation_SrcHost,  IPInboundManipulation_DestUsernamePrefix,  IPInboundManipulation_DestHost,  IPInboundManipulation_RequestType,  IPInboundManipulation_RemoveFromLeft,  IPInboundManipulation_RemoveFromRight,  IPInboundManipulation_LeaveFromRight,  IPInboundManipulation_Prefix2Add,  IPInboundManipulation_Suffix2Add;  <b>[IPInboundManipulation]</b></p> <p>For example:  IPInboundManipulation 1 = 0, 0, 0, -1, *, abc, *, *, 0, 0, 0, 255, , ;</p> <p><b>Note:</b> For a detailed description of this table, see 'Configuring IP-to-IP Inbound Manipulations' on page <a href="#">471</a>.</p>
<b>IP to IP Outbound Manipulation Table</b>	
Web: IP to IP Outbound Manipulation EMS: IP to IP Outbound Manipulation CLI: configure voip > sbc manipulations ip-outbound-manipulation <b>[IPOutboundManipulation]</b>	<p>This table parameter configures the IP to IP Outbound Manipulation table. This table allows you to manipulate the SIP URI user part (source and/or destination) of the outbound SIP dialog message. The format of this parameter is as follows:</p> <p>FORMAT IPOutboundManipulation_Index =  IPOutboundManipulation_IsAdditionalManipulation,  IPOutboundManipulation_SrcIPGroupID,  IPOutboundManipulation_DestIPGroupID,  IPOutboundManipulation_SrcUsernamePrefix,  IPOutboundManipulation_SrcHost,  IPOutboundManipulation_DestUsernamePrefix,  IPOutboundManipulation_DestHost,  IPOutboundManipulation_RequestType,  IPOutboundManipulation_ReRouteIPGroupID,  IPOutboundManipulation_Trigger,  IPOutboundManipulation_ManipulatedURI,  IPOutboundManipulation_RemoveFromLeft,  IPOutboundManipulation_RemoveFromRight,  IPOutboundManipulation_LeaveFromRight,  IPOutboundManipulation_Prefix2Add,  IPOutboundManipulation_Suffix2Add,  IPOutboundManipulation_PrivacyRestrictionMode;</p> <p>For example:  IPOutboundManipulation 1 = 0, 2, 4, "*", "*", "*", "*", 0, -1, 0, 0, 0, 0, 255, "", "", 0;</p>



Parameter	Description
	<b>Note:</b> For a detailed description of this table, see 'Configuring IP-to-IP Outbound Manipulations' on page 474.

## 59.15 Standalone Survivability Parameters

The Stand-alone Survivability (SAS) parameters are described in the table below.

### SAS Parameters

Parameter	Description
Web: Enable SAS EMS: Enable CLI: enable-sas <b>[EnableSAS]</b>	<p>Enables the Stand-Alone Survivability (SAS) feature.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>When enabled, the device receives the registration requests from different SIP entities in the local network and then forwards them to the defined proxy. If the connection to the proxy fails ('Emergency Mode'), the device serves as a proxy by allowing calls internal to the local network or outgoing to PSTN.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: SAS Local SIP UDP Port EMS: Local SIP UDP CLI: sas-local-sip-udp-port <b>[SASLocalSIPUDPPort]</b>	<p>Defines the local UDP port for sending and receiving SIP messages for SAS. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port.</p> <p>The valid range is 1 to 65,534. The default is 5080.</p>
Web: SAS Default Gateway IP EMS: Default Gateway IP CLI: sas-default-gw-ip <b>[SASDefaultGatewayIP]</b>	<p>Defines the Default Gateway used in SAS 'Emergency Mode'. When an incoming SIP INVITE is received and the destination Address-Of-Record is not included in the SAS database, the request is immediately sent to this default gateway.</p> <p>The address can be configured as an IP address (dotted-decimal notation) or as a domain name (up to 49 characters). You can also configure the IP address with a destination port, e.g., "10.1.2.3:5060". The default is a null string, i.e., the local IP address of the gateway.</p>
Web: SAS Registration Time EMS: Registration Time CLI: sas-registration-time <b>[SASRegistrationTime]</b>	<p>Defines the value of the SIP Expires header that is sent in a 200 OK response to an incoming REGISTER message when in SAS 'Emergency Mode'.</p> <p>The valid range is 0 (Analog) or 10 (Digital) to 2,000,000. The default is 20.</p>
Web: SAS Local SIP TCP Port EMS: Local SIP TCP Port CLI: sas-local-sip-tcp-port <b>[SASLocalSIPTCPPort]</b>	<p>Defines the local TCP port used to send/receive SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port.</p> <p>The valid range is 1 to 65,534. The default is 5080.</p>
Web: SAS Local SIP TLS Port EMS: Local SIP TLS Port CLI: sas-local-sip-tls-port <b>[SASLocalSIPTLSPort]</b>	<p>Defines the local TLS port used to send/receive SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port.</p> <p>The valid range is 1 to 65,534. The default is 5081.</p>

Parameter	Description
Web: SAS Connection Reuse CLI: sas-connection-reuse <b>[SASConnectionReuse]</b>	<p>Enables the re-use of the same TCP connection for sessions with the same user in the SAS application.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul> <p>The device can use the same TCP connection for multiple SIP requests / responses for a specific SIP UA. The benefits of this feature include less CPU and memory usage because fewer TCP connections are open and reduced network congestion. For example, assume the following:</p> <ul style="list-style-type: none"> <li>User A sends a REGISTER message to SAS with transport=TCP.</li> <li>User B sends an INVITE message to A using SAS.</li> </ul> <p>In this scenario, the SAS application forwards the INVITE request using the TCP connection that User A initially opened with the REGISTER message.</p>
Web/EMS: Enable Record-Route CLI: record-route <b>[SASEnableRecordRoute]</b>	<p>Determines whether the device's SAS application adds the SIP Record-Route header to SIP requests. This ensures that SIP messages traverse the device's SAS agent by including the SAS IP address in the Record-Route header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>The Record-Route header is inserted in a request by a SAS proxy to force future requests in the dialog session to be routed through the SAS agent. Each traversed proxy in the path can insert this header, causing all future dialogs in the session to pass through it as well.</p> <p>When this feature is enabled, the SIP Record-Route header includes the URI "lr" parameter, indicating loose routing, for example:</p> <pre>Record-Route: &lt;sip:server10.biloxi.com;lr&gt;</pre>
Web: SAS Proxy Set EMS: Proxy Set CLI: sas-proxy-set <b>[SASProxySet]</b>	<p>Defines the Proxy Set (index number) used in SAS Normal mode to forward REGISTER and INVITE requests from users that are served by the SAS application.</p> <p>The valid range is 0 to 5. The default is 0 (i.e., default Proxy Set).</p>
Web: Redundant SAS Proxy Set EMS: Redundant Proxy Set CLI: rdcy-sas-proxy-set <b>[RedundantSASProxySet]</b>	<p>Defines the Proxy Set (index number) used in SAS Emergency mode for fallback when the user is not found in the Registered Users database. Each time a new SIP request arrives, the SAS application checks whether the user is listed in the registration database. If the user is located in the database, the request is sent to the user. If the user is not found, the request is forwarded to the next redundant SAS defined in the Redundant SAS Proxy Set. If that SAS Proxy IP appears in the Via header of the request, it is not forwarded (thereby, preventing loops in the request's course). If no such redundant SAS exists, the SAS sends the request to its default gateway (configured by the parameter SASDefaultGatewayIP).</p> <p>The valid range is -1 to 5. The default is -1 (i.e., no redundant Proxy Set).</p>
Web/EMS: SAS Block Unregistered Users CLI: sas-block-unreg-usrs <b>[SASBlockUnRegUsers]</b>	<p>Determines whether the device rejects SIP INVITE requests received from unregistered SAS users. This applies to SAS Normal and Emergency modes.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Un-Block = (Default) Allow INVITE from unregistered SAS users.</li> <li><b>[1]</b> Block = Reject dialog-establishment requests from un-registered SAS users.</li> </ul>

Parameter	Description
CLI: sas-contact-replace <b>[SASEnableContactReplace]</b>	<p>Enables the device to change the SIP Contact header so that it points to the SAS host and therefore, the top-most SIP Via header and the Contact header point to the same host.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> (default) = Disable - when relaying requests, the SAS agent adds a new Via header (with the SAS IP address) as the top-most Via header and retains the original Contact header. Thus, the top-most Via header and the Contact header point to different hosts.</li> <li>▪ <b>[1]</b> = Enable - the device changes the Contact header so that it points to the SAS host and therefore, the top-most Via header and the Contact header point to the same host.</li> </ul> <p><b>Note:</b> Operating in this mode causes all incoming dialog requests to traverse the SAS, which may cause load problems.</p>
Web: SAS Survivability Mode EMS: Survivability Mode CLI: sas-survivability <b>[SASSurvivabilityMode]</b>	<p>Determines the Survivability mode used by the SAS application.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Standard = (Default) Incoming INVITE and REGISTER requests are forwarded to the defined Proxy list of SASProxySet in Normal mode and handled by the SAS application in Emergency mode.</li> <li>▪ <b>[1]</b> Always Emergency = The SAS application does not use Keep-Alive messages towards the SASProxySet, instead it always operates in Emergency mode (as if no Proxy in the SASProxySet is available).</li> <li>▪ <b>[2]</b> Ignore Register = Use regular SAS Normal/Emergency logic (same as option <b>[0]</b>), but when in Normal mode incoming REGISTER requests are ignored.</li> <li>▪ <b>[3]</b> Auto-answer REGISTER = When in Normal mode, the device responds to received REGISTER requests by sending a SIP 200 OK (instead of relaying the registration requests to a Proxy), and enters the registrations in its SAS database.</li> <li>▪ <b>[4]</b> Use Routing Table only in Normal mode = The device uses the IP-to-IP Routing table to route IP-to-IP SAS calls only when in SAS Normal mode (and is unavailable when SAS is in Emergency mode). This allows routing of SAS IP-to-IP calls to different destinations (and not only to the SAS Proxy Set).</li> </ul>
Web: SAS Subscribe Response CLI: sas-subscribe-resp <b>[SASSubscribeResponse]</b>	<p>Defines the SIP response upon receipt of a SUBSCRIBE message when SAS is in Emergency mode. For example, if this parameter is set to "200", then SAS sends a SIP 200 OK in response to a SUBSCRIBE message, when in Emergency mode.</p> <p>The valid value is 200 to 699. The default is 489.</p>
Web: Enable ENUM CLI: enable-enum <b>[SASEnableENUM]</b>	<p>Enables SAS to perform ENUM (E.164 number to URI mapping) queries when receiving INVITE messages in SAS emergency mode.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Web: SAS Binding Mode EMS: Binding Mode CLI: sasbindingmode <b>[SASBindingMode]</b>	<p>Determines the SAS application database binding mode.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> URI = (Default) If the incoming AoR in the INVITE requests is using a 'tel:' URI or 'user=phone' is defined, the binding is performed according to the user part of the URI only. Otherwise, the binding is according to the entire URI, i.e., User@Host.</li> <li>▪ <b>[1]</b> User Part only = The binding is always performed according to the User Part only.</li> </ul>
Web: SAS Emergency Numbers CLI: sas-emerg-nb	<p>Defines emergency numbers for the device's SAS application. When the device's SAS agent receives a SIP INVITE (from an IP phone) that includes one of the emergency numbers (in the SIP user part), it</p>

Parameter	Description
<b>[SASEmergencyNumbers]</b>	forwards the INVITE to the default gateway (configured by the parameter SASDefaultGatewayIP), i.e., the device itself, which sends the call directly to the PSTN. This is important for routing emergency numbers such as 911 (in North America) directly to the PSTN. This is applicable to SAS operating in Normal and Emergency modes.  Up to four emergency numbers can be defined, where each number can be up to four digits.
CLI: sas-emerg-prefix <b>[SASEmergencyPrefix]</b>	Defines a prefix that is added to the Request-URI user part of the INVITE message that is sent by the device's SAS agent when in Emergency mode to the default gateway or to any other destination (using the IP-to-IP Routing table). This parameter is required to differentiate between normal SAS calls routed to the default gateway and emergency SAS calls. Therefore, this allows you to define different manipulation rules for normal and emergency calls.  This valid value is a character string. The default is an empty "" string.
Web: SAS Entering Emergency Mode CLI: sas-enter-emg-mode <b>[SASEnteringEmergencyMode]</b>	Determines for which sent SIP message types the device enters SAS Emergency mode if no response is received for them from the proxy server. <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) SAS enters Emergency mode only if no response is received from sent SIP OPTIONS messages.</li> <li><b>[1]</b> = SAS enters Emergency mode if no response is received from sent SIP OPTIONS, INVITE, or REGISTER messages.</li> </ul> <b>Note:</b> If the keep-alive mechanism is disabled for the Proxy Set (in the Proxy Set table) and this parameter is set to [1], SAS enters Emergency mode only if no response is received from sent INVITE or REGISTER messages.
Web: SAS Inbound Manipulation Mode CLI: sas-inb-manipul-md <b>[SASInboundManipulationMode]</b>	Enables destination number manipulation of incoming INVITE messages when SAS is in Emergency mode. The manipulation rule is done in the IP to IP Inbound Manipulation table. <ul style="list-style-type: none"> <li><b>[0]</b> None (default)</li> <li><b>[1]</b> Emergency Only</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>Inbound manipulation applies only to INVITE requests.</li> <li>For more information on SAS inbound manipulation, see 'Manipulating Destination Number of Incoming INVITE' on page 505.</li> </ul>
<b>SAS Registration Manipulation Table</b>	
Web: SAS Registration Manipulation EMS: Stand-Alone Survivability CLI: configure voip > sas sasregistrationmanipulation <b>[SASRegistrationManipulation]</b>	This table parameter configures the SAS Registration Manipulation table. This table is used by the SAS application to manipulate the SIP Request-URI user part of incoming INVITE messages and of incoming REGISTER request AoR (To header), before saving it to the registered users database. The format of this table parameter is as follows:  <b>[SASRegistrationManipulation]</b> FORMAT SASRegistrationManipulation_Index = SASRegistrationManipulation_RemoveFromRight, SASRegistrationManipulation_LeaveFromRight; <b>[SASRegistrationManipulation]</b>  For example, the manipulation rule below routes an INVITE with Request-URI header "sip:7184002@10.33.4.226" to user "4002@10.33.4.226" (i.e., keep only four digits from right of user part):  SASRegistrationManipulation 0 = 0, 4;

Parameter	Description
	<b>Note:</b> For a detailed description of this table, see 'Manipulating URI user part of Incoming REGISTER' on page 504.
<b>Web: SAS IP-to-IP Routing Table</b>	
<b>[IP2IPRouting]</b>	<p>This table parameter configures the IP-to-IP Routing table for SAS routing rules. The format of this parameter is as follows:</p> <p><b>[IP2IPRouting]</b>            FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID, IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort, IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions;</p> <p><b>[IP2IPRouting]</b>            For example:            IP2IPRouting 1 = -1, *, *, *, *, 0, -1, -1, , 0, -1, 0;</p> <p><b>Note:</b> For a detailed description of this table parameter, see 'SAS Routing Based on IP-to-IP Routing Table' on page 508.</p>

## 59.16 IP Media Parameters

The IP media parameters are described in the table below.

**IP Media Parameters**

Parameter	Description
Web: Number of Media Channels EMS: Media Channels CLI: media-channels <b>[MediaChannels]</b>	<p>Defines the maximum number of DSP channels allocated for various functionalities (e.g., IP conferencing, IP transcoding). The default is 0.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>The SBC application does not require DSP channels. The SBC application uses DSP channels only if media transcoding is needed, where two DSP channels are used per transcoding session.</li> <li>Other DSP channels can be used for PSTN interfaces.</li> </ul>
Web: NetAnn Announcement ID <b>[NetAnnAnncID]</b>	<p>Defines the NetAnn identification string (up to 16 characters) for playing an announcement using the NetAnn interface. The application server sends a regular SIP INVITE message with a SIP URI that includes this identifier string and a "play=" parameter that identifies the necessary announcement. The default is 'annc'.</p> <p>Example 1: INVITE sip: annc@10.2.3.4;play=http://localhost/1.            Example 2: INVITE sip: annc@10.2.3.4;play=http://10.2.3.4/Annc/ello.wav.</p>
Web: Transcoding ID <b>[TranscodingID]</b>	<p>Defines the Transcoding identification string (up to 16 characters) used for identifying an incoming Transcoding call. The default is 'trans'.</p> <p>For more information on Transcoding, see NetAnn Interface.</p>

Parameter	Description
<b>Conferencing Parameters</b>	
Web/EMS: Conference ID CLI: conf-id <b>[ConferenceID]</b>	<p>Defines the Conference Identification string.</p> <p>The valid value is a string of up to 16 characters. The default is "conf".</p> <p><b>Note:</b> To join a conference, the INVITE URI must include the Conference ID string preceded by the number of the participants in the conference and terminated by a unique number. For example:</p> <pre>INVITE sip:4conf1234@10.1.10.10</pre> <p>INVITE messages with the same URI join the same conference.</p>
Web: Beep on Conference CLI: beep-on-conf <b>[BipOnConference]</b>	<p>Enables playing a beep when a participant joins or leaves a conference (in the latter case, a beep of a different pitch is heard).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul>
Web: Enable Conference DTMF Clamping CLI: conf-dtmf-clamping <b>[EnableConferenceDTMFClamp]</b>	<p>Determines the device logic once a DTMF is received on any conference participant. If enabled, the DTMF is not regenerated toward the other conference participants. This logic is only relevant for simple conferencing (NetAnn).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul>
Web: Enable Conference DTMF Reporting CLI: conf-dtmf-reporting <b>[EnableConferenceDTMFReporting]</b>	<p>Determines the device logic once a DTMF is received on any conference participant. If enabled, the device reports this DTMF in an out-of-band SIP message (according to TxDTMFOptions). This logic is only relevant for simple conferencing (NetAnn).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Web: Active Speakers Min. Interval CLI: active-speaker-notification-minimum-interval <b>[ActiveSpeakersNotificationMinInterval]</b>	<p>Defines the minimum interval (in 100 msec units) between each Active Speaker Notification (ASN) events report. These events report on the active speakers in a conference. The event is issued whenever the active speakers change.</p> <p>Minimum configurable interval between events is 500 msec (5 units). The range is 5 to 2147483647 units. The default is 20 (i.e., 100 msec).</p>
<b>Automatic Gain Control (AGC) Parameters</b>	
Web: Enable AGC EMS: AGC Enable CLI: AGC-enable <b>[EnableAGC]</b>	<p>Enables the AGC mechanism. The AGC mechanism adjusts the level of the received signal to maintain a steady (configurable) volume level.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter can also be configured in a Tel Profile.</li> <li>For a description of AGC, see Automatic Gain Control (AGC) on page 166.</li> </ul>
Web: AGC Slope EMS: Gain Slope CLI: AGC-gain-slope <b>[AGCGainSlope]</b>	<p>Determines the AGC convergence rate:</p> <ul style="list-style-type: none"> <li><b>[0]</b> 0 = 0.25 dB/sec</li> <li><b>[1]</b> 1 = 0.50 dB/sec</li> <li><b>[2]</b> 2 = 0.75 dB/sec</li> <li><b>[3]</b> 3 = 1.00 dB/sec (default)</li> <li><b>[4]</b> 4 = 1.25 dB/sec</li> <li><b>[5]</b> 5 = 1.50 dB/sec</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[6]</b> 6 = 1.75 dB/sec</li> <li>▪ <b>[7]</b> 7 = 2.00 dB/sec</li> <li>▪ <b>[8]</b> 8 = 2.50 dB/sec</li> <li>▪ <b>[9]</b> 9 = 3.00 dB/sec</li> <li>▪ <b>[10]</b> 10 = 3.50 dB/sec</li> <li>▪ <b>[11]</b> 11 = 4.00 dB/sec</li> <li>▪ <b>[12]</b> 12 = 4.50 dB/sec</li> <li>▪ <b>[13]</b> 13 = 5.00 dB/sec</li> <li>▪ <b>[14]</b> 14 = 5.50 dB/sec</li> <li>▪ <b>[15]</b> 15 = 6.00 dB/sec</li> <li>▪ <b>[16]</b> 16 = 7.00 dB/sec</li> <li>▪ <b>[17]</b> 17 = 8.00 dB/sec</li> <li>▪ <b>[18]</b> 18 = 9.00 dB/sec</li> <li>▪ <b>[19]</b> 19 = 10.00 dB/sec</li> <li>▪ <b>[20]</b> 20 = 11.00 dB/sec</li> <li>▪ <b>[21]</b> 21 = 12.00 dB/sec</li> <li>▪ <b>[22]</b> 22 = 13.00 dB/sec</li> <li>▪ <b>[23]</b> 23 = 14.00 dB/sec</li> <li>▪ <b>[24]</b> 24 = 15.00 dB/sec</li> <li>▪ <b>[25]</b> 25 = 20.00 dB/sec</li> <li>▪ <b>[26]</b> 26 = 25.00 dB/sec</li> <li>▪ <b>[27]</b> 27 = 30.00 dB/sec</li> <li>▪ <b>[28]</b> 28 = 35.00 dB/sec</li> <li>▪ <b>[29]</b> 29 = 40.00 dB/sec</li> <li>▪ <b>[30]</b> 30 = 50.00 dB/sec</li> <li>▪ <b>[31]</b> 31 = 70.00 dB/sec</li> </ul>
Web: AGC Redirection EMS: Redirection CLI: AGC-redirection <b>[AGCRedirection]</b>	<p>Determines the AGC direction.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> 0 = (Default) AGC works on signals from the TDM side.</li> <li>▪ <b>[1]</b> 1 = AGC works on signals from the IP side.</li> </ul>
Web: AGC Target Energy EMS: Target Energy CLI: AGC-target-energy <b>[AGCTargetEnergy]</b>	<p>Defines the signal energy value (dBm) that the AGC attempts to attain.</p> <p>The valid range is 0 to -63 dBm. The default is -19 dBm.</p>
EMS: Minimal Gain CLI: AGC-min-gain <b>[AGCMinGain]</b>	<p>Defines the minimum gain (in dB) by the AGC when activated.</p> <p>The range is 0 to -31. The default is -20.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: Maximal Gain CLI: AGC-max-gain <b>[AGCMaxGain]</b>	<p>Defines the maximum gain (in dB) by the AGC when activated.</p> <p>The range is 0 to 18. The default is 15.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
EMS: Disable Fast Adaptation CLI: AGC-disable-fast-adaptation <b>[AGCDisableFastAdaptation]</b>	<p>Enables the AGC Fast Adaptation mode.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Energy Detector Parameters	

Parameter	Description
Enable Energy Detector CLI: energy-detector-enable <b>[EnableEnergyDetector]</b>	Enables the Energy Detector feature. This feature generates events (notifications) when the signal received from the PSTN is higher or lower than a user-defined threshold (defined by the EnergyDetectorThreshold parameter). <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Energy Detector Quality Factor CLI: energy-detector-sensitivity <b>[EnergyDetectorQualityFactor]</b>	Defines the Energy Detector's sensitivity level. The valid range is 0 to 10, where 0 is the lowest sensitivity and 10 the highest sensitivity. The default is 4.
Energy Detector Threshold CLI: energy-detector-threshold <b>[EnergyDetectorThreshold]</b>	Defines the Energy Detector's threshold. A signal below or above this threshold invokes an 'Above' or 'Below' event. The threshold is calculated as follows: $\text{Actual Threshold} = -44 \text{ dBm} + (\text{EnergyDetectorThreshold} * 6)$ The valid value range is 0 to 7. The default is 3 (i.e., -26 dBm).
Pattern Detection Parameters <b>Note:</b> For an overview on the pattern detector feature for TDM tunneling, see DSP Pattern Detector on page <a href="#">282</a> .	
Web: Enable Pattern Detector <b>[EnablePatternDetector]</b>	Enables the Pattern Detector (PD) feature. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
<b>[PDPattern]</b>	Defines the patterns that can be detected by the Pattern Detector. The valid range is 0 to 0xFF. <b>Note:</b> For this parameter to take effect, a device reset is required.
<b>[PDThreshold]</b>	Defines the number of consecutive patterns to trigger the pattern detection event. The valid range is 0 to 31. The default is 5. <b>Note:</b> For this parameter to take effect, a device reset is required.



## 59.17 Auxiliary and Configuration File Name Parameters

The configuration files (i.e., auxiliary files) can be loaded to the device using the Web interface. For loading these files using the *ini* file, you need to configure these files in the *ini* file and configured whether they must be stored in the non-volatile memory. The table below lists the *ini* file parameters associated with these auxiliary files. For more information on the auxiliary files, see 'Loading Auxiliary Files' on page 535.

**Auxiliary and Configuration File Parameters**

Parameter	Description
<b>General Parameters</b>	
<b>[SetDefaultOnIniFileProcess]</b>	<p>Determines if all the device's parameters are set to their defaults before processing the updated <i>ini</i> file.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable - parameters not included in the downloaded <i>ini</i> file are not returned to default settings (i.e., retain their current settings).</li> <li><b>[1]</b> = Enable (default).</li> </ul> <p><b>Note:</b> This parameter is applicable only for automatic HTTP update or Web <i>ini</i> file upload (not applicable if the <i>ini</i> file is loaded using BootP).</p>
<b>[SaveConfiguration]</b>	<p>Determines if the device's configuration (parameters and files) is saved to flash (non-volatile memory).</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Configuration isn't saved to flash memory.</li> <li><b>[1]</b> = (Default) Configuration is saved to flash memory.</li> </ul>
<b>Auxiliary and Configuration File Name Parameters</b>	
Web/EMS: Call Progress Tones File <b>[CallProgressTonesFileName]</b>	<p>Defines the name of the file containing the Call Progress Tones definitions. For more information on how to create and load this file, refer to <i>DConvert Utility User's Guide</i>.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: CAS File EMS: Trunk Cas Table Index <b>[CASFileName_x]</b>	<p>Defines the CAS file name (e.g., 'E_M_WinkTable.dat'), which defines the CAS protocol (where x denotes the CAS file ID 0 to 7). It is possible to define up to eight different CAS files by repeating this parameter. Each CAS file can be associated with one or more of the device's trunks, using the parameter CASTableIndex or it can be associated per B-channel using the parameter CASChannelIndex.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Dial Plan EMS: Dial Plan Name <b>[CasTrunkDialPlanName_x]</b>	<p>Defines the Dial Plan name (up to 11-character strings) per trunk (denoted by x).</p>
Web: Dial Plan File EMS: Dial Plan File Name <b>[DialPlanFileName]</b>	<p>Defines the name (and path) of the Dial Plan file. This file should be created using AudioCodes DConvert utility (refer to <i>DConvert Utility User's Guide</i>).</p>
<b>[UserInfoFileName]</b>	<p>Defines the name (and path) of the file containing the User Information data.</p>

## 59.18 Automatic Update Parameters

The automatic update of software and configuration files parameters are described in the table below.

**Automatic Update of Software and Configuration Files Parameters**

Parameter	Description
<b>General Automatic Update Parameters</b>	
<b>[AutoUpdateCmpFile]</b>	<p>Enables the Automatic Update mechanism for the cmp file.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) The Automatic Update mechanism doesn't apply to the cmp file.</li> <li><b>[1]</b> = The Automatic Update mechanism includes the cmp file.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[AutoUpdateFrequency]</b>	<p>Defines the number of minutes that the device waits between automatic updates. The default is 0 (i.e., the update at fixed intervals mechanism is disabled).</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[AutoUpdatePredefined Time]</b>	<p>Defines schedules (time of day) for automatic updates. The format of this parameter is: 'HH:MM', where <i>HH</i> denotes the hour and <i>MM</i> the minutes, for example, 20:18.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>The actual update time is randomized by five minutes to reduce the load on the Web servers.</li> </ul>
EMS: AUPD Verify Certificates CLI: system/tls/aupd-verify-cert <b>[AUPDVerifyCertificates]</b>	<p>Determines whether the Automatic Update mechanism verifies server certificates when using HTTPS.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul>
<b>[AUPDCheckIfIniChanged]</b>	<p>Determines whether the Automatic Update mechanism performs CRC checking to determine if the <i>ini</i> file has changed prior to processing.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Do not check CRC. The <i>ini</i> file is loaded whenever the server provides it.</li> <li><b>[1]</b> = Check CRC for the entire file. Any change, including line order, causes the <i>ini</i> file to be re-processed.</li> <li><b>[2]</b> = Check CRC for individual lines. Use this option when the HTTP server scrambles the order of lines in the provided <i>ini</i> file.</li> </ul>
CLI: auto-update-use-zero-conf-certs <b>[AupdUseZeroConfCertificates]</b>	<p>Enables the Automatic Update feature to use the same client-server certificate as used for the Zero Configuration feature, instead of the "regular" certificate used for Automatic Update.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) The device uses the "regular" certificate for Automatic Update.</li> <li><b>[1]</b> = The device uses the Zero Configuration certificate for the Automatic Update feature.</li> </ul>
<b>[ResetNow]</b>	<p>Invokes an immediate device reset. This option can be used to activate offline (i.e., not on-the-fly) parameters that are loaded using the parameter IniFileUrl.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) The immediate restart mechanism is disabled.</li> <li><b>[1]</b> = The device immediately resets after an <i>ini</i> file with this parameter set to 1 is loaded.</li> </ul>

Parameter	Description
<b>Software/Configuration File URL Path for Automatic Update Parameters</b>	
CLI: firmware <b>[CmpFileURL]</b>	<p>Defines the name of the <i>cmp</i> file and the path to the server (IP address or FQDN) from where the device can load the <i>cmp</i> file and update itself. The <i>cmp</i> file can be loaded using HTTP/HTTPS. For example: <code>http://192.168.0.1/filename</code></p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>When this parameter is configured, the device always loads the <i>cmp</i> file after it is reset.</li> <li>The <i>cmp</i> file is validated before it's burned to flash. The checksum of the <i>cmp</i> file is also compared to the previously burnt checksum to avoid unnecessary resets.</li> <li>The maximum length of the URL address is 255 characters.</li> </ul>
CLI: voice-configuration <b>[IniFileURL]</b>	<p>Defines the name of the <i>ini</i> file and the path to the server (IP address or FQDN) on which it is located. The <i>ini</i> file can be loaded using HTTP/HTTPS. For example: <code>http://192.168.0.1/filename</code> <code>http://192.8.77.13/config&lt;MAC&gt;</code> <code>https://&lt;username&gt;:&lt;password&gt;@&lt;IP address&gt;/&lt;file name&gt;</code></p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>When using HTTP or HTTPS, the date and time of the <i>ini</i> file are validated. Only more recently dated <i>ini</i> files are loaded.</li> <li>The optional string &lt;MAC&gt; is replaced with the device's MAC address. Therefore, the device requests an <i>ini</i> file name that contains its MAC address. This option allows the loading of specific configurations for specific devices.</li> <li>The maximum length of the URL address is 99 characters.</li> </ul>
CLI: copy cli-script from <URL> <b>[AUPDCliScriptURL]</b>	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.
CLI: copy startup-script from <URL> <b>[AUPDStartupScriptURL]</b>	Defines the URL of the server where the CLI Startup Script file containing the device's configuration is located. This file is used for automatic provisioning.
CLI: call-progress-tones <b>[CptFileURL]</b>	<p>Defines the name of the CPT file and the path to the server (IP address or FQDN) on which it is located. For example: <code>http://server_name/file</code>, <code>https://server_name/file</code>.</p> <p><b>Note:</b> The maximum length of the URL address is 99 characters.</p>
CLI: cas-table <b>[CasFileURL]</b>	<p>Defines the name of the CAS file and the path to the server (IP address or FQDN) on which it is located. For example: <code>http://server_name/file</code>, <code>https://server_name/file</code>.</p> <p><b>Note:</b> The maximum length of the URL address is 99 characters.</p>
CLI: tls-root-cert <b>[TLSRootFileUrl]</b>	<p>Defines the name of the TLS trusted root certificate file and the URL from where it can be downloaded.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>

Parameter	Description
CLI: tls-cert [TLSCertFileUrl]	Defines the name of the TLS certificate file and the URL from where it can be downloaded. <b>Note:</b> For this parameter to take effect, a device reset is required.
CLI: tls-private-key [TLSPkeyFileUrl]	Defines the URL for downloading a TLS private key file using the Automatic Update facility.
[UserInfoFileURL]	Defines the name of the User Information file and the path to the server (IP address or FQDN) on which it is located. For example: http://server_name/file, https://server_name/file <b>Note:</b> The maximum length of the URL address is 99 characters.

## 60 DSP Templates

The device supports the following DSP firmware capabilities.


**Notes:**

- Installation and use of voice coders is subject to obtaining the appropriate license and royalty payments.
- For additional DSP templates, contact your AudioCodes representative.

### Channel Capacity and Capabilities

Telephony Interface Assembly	DSP Channels on Physical Interface	SBC Enhancements	Advanced DSP Capabilities							SBC Sessions
			IPM Detectors	AMR WB	SILK	SILK WB	V.150.1	Transcoding Sessions	Conference Participants	
2 x E1/T1	60 / 48	-	-	-	-	-	-	0 / 6	-	0 / 12
2 x T1	48	-	Yes	-	Yes	-	Yes	0	-	12
1 x E1/T1 & FXS / FXO Mix x 8	38 / 32	-	Yes	-	-	-	-	4 / 7	-	22 / 28
	38 / 32	-	Yes	-	Yes	-	-	3 / 6	-	22 / 28
1 x E1/T1	30 / 24	-	Yes	-	Yes	-	Yes	7 / 9	-	30 / 36
4 x BRI & 4 x FXS & 4 x FXO	16	-	Yes	-	Yes	-	-	0	-	48
8 x BRI	16	-	Yes	-	Yes	-	-	0	-	44
12 x FXS	12	-	Yes	-	Yes	-	Yes	1	-	48
4 x FXS & 8 x FXO	12	-	Yes	-	Yes	-	-	1	-	48
4 x BRI & 4 x FXS	12	-	Yes	-	Yes	-	-	1	-	48
4 x FXS & 4 x FXO	8	-	-	-	-	-	-	4	6	52
	8	-	Yes	-	Yes	-	-	3	-	52
4 x BRI	8	-	-	-	-	-	-	4	6	52
	8	-	Yes	-	Yes	-	-	3	-	52
4 x FXS or 4 x FXO	4	-	-	-	Yes	-	Yes	6	-	56
	4	-	-	-	-	-	-	5	8	56
	4	-	-	-	Yes	-	-	3	7	56
	4	-	Yes	Yes	Yes	-	-	2	4	56

Telephony Interface Assembly	DSP Channels on Physical Interface	SBC Enhancements	Advanced DSP Capabilities							SBC Sessions
			IPM Detectors	AMR WB	SILK	SILK WB	V.150.1	Transcoding Sessions	Conference Participants	
	4	-	Yes	Yes	Yes	Yes	-	2	4	56
SBC (Telephony Interfaces may be Present, but are Inactive)	-	-	-	-	-	-	-	11	-	60
Without Telephony Interfaces	-	-	-	-	-	-	-	30	-	60
	-	Yes	-	-	-	-	-	25	-	60
	-	-	-	-	Yes	-	-	21	-	60
	-	-	-	Yes	Yes	Yes	-	18	-	60
	-	Yes	-	-	Yes	-	-	16	-	60
	-	Yes	-	Yes	Yes	Yes	-	13	-	60

**Notes:**

- For availability of the telephony assemblies listed in the table above, please contact your AudioCodes sales representative.
- All hardware assemblies also support the following DSP channel capabilities: IBS, echo cancellation (EC), CID (caller ID), silence compression (SC), T.38, G.711, G.726, G.729, G.723.1, G.722, AMR, RTCP XR reporting, SRTP.
- SBC enhancements include the network Acoustic Echo Suppressor.
- IPM Detectors include Automatic Gain Control (AGC) and Answer Detector (AD).
- V.150.1 is supported only for the US Department of Defense (DoD).
- Transcoding Sessions are part of the total SBC Sessions.
- The Conference Participants column lists the number of participants in one or more conference (bridge), where each conference may include three or more participants. Conferences are supported on all above configurations. Please contact AudioCodes for the maximum number of participants per configuration.



## 61 Technical Specifications

The device's technical specifications are listed in the table below.



### Notes:

- All specifications in this document are subject to change without prior notice.
- The compliance and regulatory information can be downloaded from AudioCodes Web site at <http://www.audiocodes.com/library>.

### Technical Specifications

Function	Specification
<b>Capacity</b>	
<b>SBC Sessions</b>	<ul style="list-style-type: none"> <li>▪ RTP-RTP: 60</li> <li>▪ SRTP-RTP: 60</li> </ul>
<b>IP-to-IP Transcoding Sessions</b>	30
<b>Registered Users (SAS/SBC/CRP/)</b>	200
<b>Telephony Interfaces</b>	
<b>PRI Interfaces</b>	Single E1/T1 span, using RJ-48c ports
<b>BRI Interfaces</b>	Up to 8 BRI ports (16 calls), network S/T interfaces - NT or TE termination
<b>Analog Interfaces</b>	<ul style="list-style-type: none"> <li>▪ Up to 12 FXS, using RJ-11 ports</li> <li>▪ Up to FXO ports, using RJ-11 ports</li> <li>▪ (Option) 1 FXS Lifeline ports in case of power failure</li> <li>▪ FXS Loop Impedance - Up to 1,600 Ohms</li> </ul>
<b>Networking Interfaces</b>	
<b>WAN</b>	<ul style="list-style-type: none"> <li>▪ Copper 1000Base-T (Gigabit Ethernet) using RJ-45 port</li> <li>▪ SHDSL using RJ-11 ports</li> <li>▪ ADSL2+/VDSL2 using RJ-11 ports</li> <li>▪ 3G Cellular (primary or backup) using USB modem</li> </ul>
<b>LAN</b>	<ul style="list-style-type: none"> <li>▪ 4 Gigabit Ethernet (10/100/1000Base-T) using RJ-45 ports</li> <li>▪ 8 Fast Ethernet (FE) 10/100Base-TX ports using RJ-45 ports</li> <li>▪ Power-over-Ethernet (PoE) on all ports is optional, compliant to 802.3af-2003 with auto-detection, supporting up to 15.4W per port respectively. PoE management</li> </ul>
<b>Wi-Fi</b>	<ul style="list-style-type: none"> <li>▪ Wireless LAN 802.11 b/g/n access point at 2.4 and 5 GHz, integrated 2 Tx and 2 Rx, enabling data rates of up to 300 Mbps</li> <li>▪ 2 Wi-Fi antennas</li> </ul>
<b>USB</b>	1 USB port for optional, 3G cellular WAN modem and/or USB storage services
<b>Media Processing</b>	
<b>Voice Coders</b>	G.711, G.722, G.723.1, G.726, G.729A, and AMR-WB (G.722.2)

Function	Specification
	Independent dynamic vocoder selection per channel
<b>Echo Cancellation</b>	G.165 and G.168-2002, with 32, 64 or 128 msec tail length
<b>Quality Enhancement</b>	Dynamic programmable jitter buffer, VAD, CNG
<b>DTMF/MF Tones</b>	Packet-side or PSTN-side detection and generation, RFC 2833 compliant DTMF relay and Call Progress tones Detection and Generation
<b>IP Transport</b>	VoIP (RTP/RTCP) per IETF RFC 3550 and 3551, IPv6
<b>Fax Transport</b>	T.38 compliant (real time fax), Automatic bypass to PCM
<b>Signaling</b>	
<b>Digital PSTN Protocols</b>	<ul style="list-style-type: none"> <li>E1/T1: <ul style="list-style-type: none"> <li>✓ PRI: ETSI/Euro ISDN, ANSI NI-2, 4/5ESS, DMS-100, QSIG (basic and supplementary), Japan INS1500, VN3, VN4, VN6, Australian Telecom, New Zealand Telecom, Hong Kong Variant, Korean Variant</li> <li>✓ CAS: <ul style="list-style-type: none"> <li>- T1 CAS (protocol type 2) (MF-R1\DTMF) – supports various variants supplied as state machine such as E&amp;M family, E911CAMA, Loop\Ground Start</li> <li>- E1 MFCR2 (protocol type 7) – supports various countries supplied as state machine</li> <li>- E1 CAS (protocol type 8) (MF-R2\MF-R1\DTMF) – supports R2D variant supplied as state machine</li> <li>- E1\T1 RAW CAS (protocol type 3 and 9 accordingly)</li> <li>- Customized state machine</li> </ul> </li> </ul> </li> <li>BRI: 8 BRI ports (16 calls) with S/T interfaces. Supports Euro ISDN, QSIG, VN6 and NTT</li> </ul>
<b>Analog</b>	Loop Start FXS/FXO, Caller ID, polarity reversal, distinctive ringing, visual Message Waiting Indication
<b>OSN Server Platform (Optional)</b>	
<b>Single Chassis Integration</b>	<p>Embedded, open Network Solution Platform for third-party services:</p> <ul style="list-style-type: none"> <li>OSN1: Intel® Atom™ 1.6 GHz processor, with 1GB or 2GB RAM and a single storage hard disk drive (SATA storage)</li> <li>OSN2: Intel® Celeron® 847E (2x 1.1 GHz), 2 MB L2 Cache, Intel® HM65 Second Generation</li> </ul>
<b>Data Routing (Optional)</b>	
	<ul style="list-style-type: none"> <li>PPPoE/L2TP client toward WAN</li> <li>DHCP client toward WAN, supporting the following DHCP Options: 12 Host Name; 15 Domain Name; 50 Requested IP Address; 53 DHCP Message Type; 54 DHCP Server Identifier; 55 Parameter Request List; 60 Vendor Class-identifier (e.g. ACS details); 121 Classless Static Routes.</li> <li>DHCP server toward LAN, supporting the following DHCP Options: 1 Subnet Mask; 3 Default Gateway (Router); 6 Domain Name Server; 12 Host Name; 15 Domain Name; 42 NTP Server; 43 Vendor Specific Information; 51 Lease Time; 66 TFTP server name; 67 Bootfile name; 120 SIP server (RFC 3361); 121 Classless static routes; 150 TFTP server address.</li> <li>VLAN</li> <li>Layer 3 routing</li> <li>Internal layer 2 switching</li> </ul>



Function	Specification
	<ul style="list-style-type: none"> <li>Static and dynamic routing (RIP1, RIP2, OSPF, BGP)</li> </ul>
<b>Control and Management</b>	
<b>Control Protocols</b>	SIP-TCP, SIP-UDP, SIP-TLS and SIP-MSMML* Cloud Resilience Package (CRP) and Standalone Survivability (SAS) for service continuity
<b>Operations &amp; Management</b>	<ul style="list-style-type: none"> <li>AudioCodes' Element Management System (EMS)</li> <li>Embedded HTTP Web Server, SNMP V2/V3</li> <li>Telnet, SSH, TR-069</li> <li>Remote configuration and software download via HTTP/S, RADIUS, Syslog (for events and alarms)</li> </ul>
<b>IP/VoIP Quality of Service</b>	
	<ul style="list-style-type: none"> <li>IEEE 802.1P, TOS, DiffServ labeling</li> <li>IEEE 802.1Q VLAN tagging</li> <li>RTCP XR (Extended Reports per RFC 3611)</li> <li>Shaping Policing, Queuing, Bandwidth Reservation (Optional)</li> </ul>
<b>Security</b>	
<b>Session Border Controller (SBC)</b>	<ul style="list-style-type: none"> <li>SIP Header conversion</li> <li>SIP Normalization</li> <li>Survivability</li> <li>IP-to-IP routing translations of various SIP transport types; UDP, TCP, TLS</li> <li>Translation of RTP, SRTP</li> <li>Support SIP trunk with multi-ITSP (Registrations to ITSPs is invoked independently)</li> <li>Topology hiding</li> <li>Call Admission Control</li> <li>Call Black/White list</li> </ul>
<b>Data Security (Optional)</b>	<ul style="list-style-type: none"> <li>IPsec</li> <li>ESP – Tunnel mode</li> <li>Encryption</li> <li>Authentication</li> <li>IKE mode – IPsec VPN</li> <li>IDS/IPS:               <ul style="list-style-type: none"> <li>✓ Fragmented traffic</li> <li>✓ Malformed Request</li> <li>✓ Ping of Death</li> <li>✓ Properly formed request from unauthenticated source</li> <li>✓ DDoS attack</li> <li>✓ SYN flood</li> </ul> </li> <li>Stateful packet inspection firewall</li> <li>DMZ Host</li> <li>Port Triggering</li> <li>Packet Filtering</li> <li>Application Layer Gateway</li> </ul>
<b>Data-Routing Features</b>	
<b>LAN Switching</b>	<ul style="list-style-type: none"> <li>802.1Q for VLAN tagging</li> </ul>

Function	Specification
	<ul style="list-style-type: none"> <li>▪ Rapid Spanning Tree Protocol / RSTP (802.1D-2004 and 802.1w)</li> <li>▪ LAN switch ports with non-blocking switching performance</li> <li>▪ Up to four RJ-45 10/100/1000Base-T (Gigabit Ethernet) LAN ports</li> <li>▪ Eight RJ-45 10/100Base-TX (Fast Ethernet) LAN ports</li> <li>▪ Power-over-Ethernet (PoE) supported on all LAN ports, complying with IEEE 802.3af-2003 (15.4W maximum wattage per port; 120 total wattage over all ports)</li> <li>▪ LAN ports supporting half- and full-duplex modes, auto-negotiation, and straight or crossover cable detection.</li> </ul>
<b>Routing</b>	<ul style="list-style-type: none"> <li>▪ Dynamic Host Configuration Protocol (DHCP): <ul style="list-style-type: none"> <li>✓ DHCP server, DHCP relay and DHCP client</li> <li>✓ DHCP server supports fixed binding of IP-to-MAC address</li> <li>✓ DHCP server supports user-defined DNS server allocation</li> </ul> </li> <li>▪ Multiple IP interfaces for LAN routing: IP interfaces assignment to different VLANs</li> <li>▪ Assignment of different VLAN IDs to VoIP and Data traffic</li> <li>▪ Symmetric High-Speed Digital Subscriber Line (SHDSL): <ul style="list-style-type: none"> <li>✓ ATM: RFC 2684 over AAL5 with LLC-SNAP and VC-MUX over AAL5; ATM UNI 4.1; UBR, CBR, VBR-RT and VBR-NRT; IP QoS; Multiple IP interfaces; RFC 2684 Routed Mode; RFC 2364 PPPoA; RFC 2516 PPPoE over ATM; Up to 8 PVCs</li> <li>✓ EFM: ITU G.991.2 Annex E for Ethernet, also known as EFM or 2Base-TL, as defined in IEEE 802.3ah; Up to 8 IP interfaces for EFM/2Base-TL; IP QoS classification, Marking, scheduling and shaping; 802.1Q VLANs</li> </ul> </li> <li>▪ Routing protocols: <ul style="list-style-type: none"> <li>✓ Static routing</li> <li>✓ RIPv1 - RFC 1058</li> <li>✓ RIPv2 - RFC 2453</li> <li>✓ OSPFv2 - RFC 2328</li> <li>✓ BGPv4 - RFC 1771 and RFC 2858</li> <li>✓ BGP Extended Community Attribute for BGP/MPLS VPNs</li> <li>✓ Policy-based routing (e.g. DSCP-based and BGP policy routing)</li> </ul> </li> <li>▪ Network Address Translation (NAT/NAPT): <ul style="list-style-type: none"> <li>✓ ACL-like classification with ALG support</li> <li>✓ Source and destination-based IP addresses ACLs</li> <li>✓ Multiple NAT and NAPT WAN addresses</li> </ul> </li> <li>▪ WAN access via PPPoE, L2TP, DHCP</li> <li>▪ Quality of service (QoS): <ul style="list-style-type: none"> <li>✓ Traffic Classification and Marking: Connection-based (with SPI) or packet-based classification; VoIP classification for SIP signaling and media traffic (tracking UDP ports selected by SDP offer-answer negotiations); DSCP and 802.1p marking; Explicit classification criteria (source/destination MAC and IP addresses; Protocol ALG-based; L4 port numbers DSCP/802.1p; Length of packets or their data portion only)</li> <li>✓ Traffic scheduling and shaping: Ingress traffic policing; Traffic reservation - when not utilized, other classes are served with extra bandwidth; Maximum egress traffic shaping; Scheduling (Strict Priority, Fair, Weighted Round-Robin Queuing, and Class-Based WRR Queuing); Queue management (RED; TCP Serialization Reduction to minimize jitter in VoIP environments)</li> </ul> </li> </ul>
<b>Data Security</b>	<ul style="list-style-type: none"> <li>▪ Access Control for pinpoint security policy</li> </ul>

Function	Specification
	<ul style="list-style-type: none"> <li>▪ Extensive list of ALG-modules combined with SPI for error-free configuration and maximum security</li> <li>▪ Port-forwarding and DMZ support for local applications and hosts</li> <li>▪ Website Restriction allows static URL-based blocking of public/extranet websites</li> <li>▪ Advanced Filtering allows full control on Inbound/Outbound Rules per interface/device</li> <li>▪ Site-to-Site VPN: <ul style="list-style-type: none"> <li>✓ Supports two IPSec use-cases: Site-to-Site Gateway-to-Gateway) VPN; Teleworker (User-to-Gateway) VPN</li> <li>✓ Fully compliant with IPSec RFCs: RFC 2401 - Security Architecture for IP; RFC 2402 - IP Authentication Header; RFC 2406 – ESP; RFC 2403 and RFC 2404 for Authentication</li> </ul> </li> <li>▪ L2TP Client-Server VPN: <ul style="list-style-type: none"> <li>✓ Supports two VPN use-cases: Server support for remote Teleworker VPN access; Client-to-Gateway support with L2TP</li> <li>✓ Layer Two Tunneling Protocol - RFC 2661 (with L2TP/IPSec)</li> <li>✓ Support all WiN OS versions as well as Linux</li> </ul> </li> <li>▪ DoS and IDS/IPS: <ul style="list-style-type: none"> <li>✓ Denial of Service (DoS) protection: TCP RST, Ping Flood, ICMP Echo storm, UDP snork attack, ICMP Smurf, UDP fraggle and more</li> <li>✓ IP spoofing attacks: FTP bounce, Broadcast/multicast source IP attack</li> <li>✓ Intrusion and scanning attacks: IP source route, ICMP Echo reply without request, ICMP Ping sweep, TCP Stealth; Scan (FIN, XMAS, NULL), UDP port, FTP passive attack, loopback / Echo chargen, Block security hazard ICMP messages</li> <li>✓ IP fragment overlap, Ping of Death, Fragmentation attacks and more</li> </ul> </li> </ul>
<b>Supported RFCs</b>	<ul style="list-style-type: none"> <li>▪ IP/Routing: <ul style="list-style-type: none"> <li>✓ RFC 768 UDP</li> <li>✓ RFC 791 IP</li> <li>✓ RFC 792 ICMP</li> <li>✓ RFC 793 TCP</li> <li>✓ RFC 959 FTP</li> <li>✓ RFC 2822 Internet Message Format</li> <li>✓ RFC 1305 NTP</li> <li>✓ RFC 826 ARP</li> <li>✓ RFC 2131 DHCP</li> <li>✓ RFC 1918 IP Addressing</li> <li>✓ RFC 2516 PPPoE</li> <li>✓ RFC 2663 NAT</li> </ul> </li> <li>▪ QoS: <ul style="list-style-type: none"> <li>✓ IEEE 802.1p Priority Tagging</li> <li>✓ RFC 1349</li> <li>✓ RFC 2475</li> <li>✓ RFC 2597</li> <li>✓ RFC 3246</li> </ul> </li> <li>▪ IPSec: <ul style="list-style-type: none"> <li>✓ RFC 2401 Security Architecture for IP</li> <li>✓ RFC 2402 AH - IP Authentication Header</li> <li>✓ RFC 2403 IPsec Authentication - MD5</li> <li>✓ RFC 2404 IPsec Authentication - SHA-1</li> <li>✓ RFC 2405 IPsec Encryption - DES</li> </ul> </li> </ul>

Function	Specification
	<ul style="list-style-type: none"><li>✓ RFC 2406 ESP - IPsec Encryption</li><li>✓ RFC 2407 IPsec DOI</li><li>✓ RFC 2408 ISAKMP</li><li>✓ RFC 2409 IKE</li><li>✓ RFC 2410 IPsec Encryption – NULL</li><li>✓ RFC 2411</li><li>✓ RFC 2412 OAKLEY</li></ul>
<b>Hardware Specifications</b>	
<b>Power Supply</b>	Single universal AC power supply 100-240V, 1.5A, 50-60 Hz
<b>Physical Dimensions</b>	32 x 34.5 cm (12.6 x 13.6 inches) x 1U
<b>Weight</b>	2.5 kg (5.5 lb)

## Reader's Notes



User's Manual Ver. 6.6