MediaPack™ MP-11x & MP-124

VoIP Media Gateway

SIP Protocol

User's Manual

Version 6.2

February 2011

Document # LTRT-65415

AudioCodes

Table of Contents

1 Overview 21

1.1 Gateway Description 21
1.2 MediaPack Features 23
1.2.1 MP-11x Hardware Features 23
1.2.2 MP-124 Hardware Features 23
1.3 SIP Overview 24

2 Configuration Tools 25

3 Web-Based Management 27

3.1 Getting Acquainted with the Web Interface 28
3.1.1 Computer Requirements 28
3.1.2 Accessing the Web Interface 28
3.1.3 Areas of the GUI 30
3.1.4 Toolbar 31
3.1.5 Navigation Tree 32
3.1.5.1 Displaying Navigation Tree in Basic and Full View 33
3.1.5.2 Showing / Hiding the Navigation Pane 34
3.1.6 Working with Configuration Pages 35
3.1.6.1 Accessing Pages 35
3.1.6.2 Viewing Parameters 35
3.1.6.3 Modifying and Saving Parameters 37
3.1.6.4 Entering Phone Numbers 38
3.1.6.5 Working with Tables 39
3.1.7 Searching for Configuration Parameters 40
3.1.8 Working with Scenarios 41
3.1.8.1 Creating a Scenario 42
3.1.8.2 Accessing a Scenario 44
3.1.8.3 Editing a Scenario 45
3.1.8.4 Saving a Scenario to a PC 47
3.1.8.5 Loading a Scenario to the Device 48
3.1.8.6 Deleting a Scenario 48
3.1.8.7 Exiting Scenario Mode 49
3.1.9 Creating a Login Welcome Message 50
3.1.10 Getting Help 51
3.1.11 Logging Off the Web Interface 52
3.2 Using the Home Page 53
3.2.1 Assigning a Port Name 55
3.2.2 Resetting an Analog Channel 55
3.2.3 Viewing Analog Port Information 56
3.3 Configuration Tab 57
3.3.1 System Settings 57
3.3.1.1 Configuring Application Settings 58
3.3.1.2 Configuring NFS Settings 59
3.3.1.3 Configuring Syslog Settings 61
3.3.1.4 Configuring Regional Settings 62
3.3.1.5 Configuring Certificates 62
3.3.1.6 Management Settings 66
3.3.2 VoIP Settings 78
3.3.2.1 Network 78
3.3.2.2 Security 89
3.3.2.3 Media 98
3.3.2.4 Applications Enabling 102
3.3.2.5 Control Network 103

3.3.2.6 SIP Definitions 110
3.3.2.7 Coders and Profiles 117
3.3.2.8 GW and IP to IP 124
3.3.2.9 SAS 161
3.4 Maintenance Tab 166
3.4.1 Maintenance 166
3.4.1.1 Maintenance Actions 166
3.4.2 Software Update 170
3.4.2.1 Loading Auxiliary Files 170
3.4.2.2 Loading Software Upgrade Key 172
3.4.2.3 Software Upgrade Wizard 175
3.4.2.4 Backing Up and Loading Configuration File 178
3.5 Status & Diagnostics Tab 180
3.5.1 System Status 180
3.5.1.1 Viewing Syslog Messages 180
3.5.1.2 Viewing Device Information 182
3.5.1.3 Viewing Ethernet Port Information 182
3.5.1.4 Carrier-Grade Alarms 183
3.5.2 VoIP Status 184
3.5.2.1 Viewing Active IP Interfaces 184
3.5.2.2 Viewing Performance Statistics 184
3.5.2.3 Viewing Call Counters 185
3.5.2.4 Viewing SAS/SBC Registered Users 187
3.5.2.5 Viewing Call Routing Status 188
3.5.2.6 Viewing Registration Status 189
3.5.2.7 Viewing IP Connectivity 190
4 INI File-Based Management 193
4.1 INI File Format 193
4.1.1 Configuring Individual ini File Parameters 193
4.1.2 Configuring ini File Table Parameters 194
4.1.3 General ini File Formatting Rules 196
4.2 Modifying an ini File 196
4.3 Secured Encoded ini File 197
5 EMS-Based Management 199
5.1 Familiarizing yourself with EMS GUI 199
5.2 Securing EMS-Device Communication 200
5.2.1 Configuring IPSec 200
5.2.2 Changing SSH Login Password 201
5.3 Adding the Device in EMS 202
5.4 Configuring Basic SIP Parameters 204
5.5 Configuring Advanced IPSec/IKE Parameters 205
5.6 Provisioning SIP SRTP Crypto Offered Suites 206
5.7 Provisioning SIP MLPP Parameters 207
5.8 Configuring the Device to Operate with SNMPv3 208
5.8.1 Configuring SNMPv3 using SSH 208
5.8.2 Configuring EMS to Operate with a Pre-configured SNMPv3 System 209
5.8.3 Configuring SNMPv3 to Operate with Non-Configured SNMPv3 System 210
5.8.4 Cloning SNMPv3 Users 211
5.9 Resetting the Device 211
5.10 Upgrading the Device's Software 212

6 Restoring Factory Default Settings 215

6.1 Restoring Defaults using CLI 215
6.2 Restoring Defaults using an ini File 216
6.3 Restoring Defaults using Hardware Reset Button 216

7 Auxiliary Configuration Files 217

7.1 Call Progress Tones File 217
7.1.1 Distinctive Ringing 220
7.1.2 FXS Distinctive Ringing and Call Waiting Tones per Source/Destination Number 221
7.2 Prerecorded Tones File 222
7.3 Dial Plan File 223
7.4 User Information File 224

8 IP Telephony Capabilities 227

8.1 Dynamic Jitter Buffer Operation 227
8.2 Gateway and IP-to-IP 228
8.2.1 Dialing Plan Features 228
8.2.1.1 Dialing Plan Notation for Routing and Manipulation 228
8.2.1.2 Digit Mapping 229
8.2.1.3 External Dial Plan File 230
8.2.2 Manipulating Number Prefix 232
8.2.3 Configuring DTMF Transport Types 233
8.2.4 FXS and FXO Capabilities 234
8.2.4.1 FXS/FXO Coefficient Types 234
8.2.4.2 FXO Operating Modes 234
8.2.4.3 Remote PBX Extension Between FXO and FXS Devices 242
8.2.5 Configuring Alternative Routing (Based on Connectivity and QoS) 247
8.2.5.1 Alternative Routing Mechanism 247
8.2.5.2 Determining the Availability of Destination IP Addresses 247
8.2.6 Fax and Modem Capabilities 248
8.2.6.1 Fax/Modem Operating Modes 248
8.2.6.2 Fax/Modem Transport Modes 248
8.2.6.3 V.152 Support 253
8.2.6.4 Fax Transmission behind NAT 254
8.2.7 Working with Supplementary Services 254
8.2.7.1 Call Hold and Retrieve 255
8.2.7.2 Call Pickup 257
8.2.7.3 Consultation Feature 257
8.2.7.4 Call Transfer 258
8.2.7.5 Call Forward 259
8.2.7.6 Call Waiting 261
8.2.7.7 Message Waiting Indication 262
8.2.7.8 Caller ID 262
8.2.7.9 Three-Way Conferencing 265
8.2.7.10 Multilevel Precedence and Preemption 266
8.2.8 SIP Call Routing Examples 268
8.2.8.1 SIP Call Flow Example 268
8.2.8.2 SIP Authentication Example 271
8.2.8.3 Establishing a Call between Two Devices 274
8.2.8.4 SIP Trunking between Enterprise and ITSPs 275
8.2.9 Mapping PSTN Release Cause to SIP Response 278
8.2.10 Querying Device Channel Resources using SIP OPTIONS 278
8.3 Stand-Alone Survivability (SAS) Application 279
8.3.1 SAS Operating Modes 279

8.3.1.1 SAS Outbound Mode 280
8.3.1.2 SAS Redundant Mode 282
8.3.2 SAS Routing 284
8.3.2.1 SAS Routing in Normal State 284
8.3.2.2 SAS Routing in Emergency State 286
8.3.3 SAS Configuration 287
8.3.3.1 General SAS Configuration 287
8.3.3.2 Configuring SAS Outbound Mode 290
8.3.3.3 Configuring SAS Redundant Mode 291
8.3.3.4 Configuring Gateway Application with SAS 291
8.3.3.5 Advanced SAS Configuration 295
8.3.4 Viewing Registered SAS Users 300
8.4 General 301
8.4.1 Event Notification using X-Detect Header 301
8.4.2 Supported RADIUS Attributes 304
8.4.3 Call Detail Record 306
8.4.3.1 CDR Fields 306
8.4.3.2 Release Reasons in CDR 308
8.4.4 RTP Multiplexing (ThroughPacket) 310
9 VoIP Networking Capabilities 311
9.1 Ethernet Interface Configuration 311
9.2 NAT (Network Address Translation) Support 311
9.2.1 STUN 312
9.2.2 First Incoming Packet Mechanism 313
9.2.3 No-Op Packets 313
9.3 IP Multicasting 314
9.4 Robust Receipt of Media Streams 314
9.5 Multiple Routers Support 314
9.6 Simple Network Time Protocol Support 315
9.7 Network Configuration 316
9.7.1 Multiple Network Interfaces and VLANs 316
9.7.1.1 Overview of Multiple Interface Table 317
9.7.1.2 Columns of the Multiple Interface Table 317
9.7.1.3 Other Related Parameters 320
9.7.1.4 Multiple Interface Table Configuration Summary and Guidelines 323
9.7.1.5 Troubleshooting the Multiple Interface Table 324
9.7.2 Static Routing Table 325
9.7.2.1 Routing Table Overview 325
9.7.2.2 Routing Table Columns 325
9.7.2.3 Routing Table Configuration Summary and Guidelines 326
9.7.2.4 Troubleshooting the Routing Table 327
9.7.3 Setting Up VoIP Networking 328
9.7.3.1 Using the Web Interface 328
9.7.3.2 Using the ini File 328
9.7.3.3 Networking Configuration Examples 329
10 Configuration Parameters Reference 333
10.1 Networking Parameters 333
10.1.1 Ethernet Parameters 333
10.1.2 Multiple Network Interfaces and VLAN Parameters 334
10.1.3 Static Routing Parameters 337
10.1.4 Quality of Service Parameters 337
10.1.5 NAT and STUN Parameters 339
10.1.6 NFS Parameters 341
10.1.7 DNS Parameters 342

10.1.8 DHCP Parameters 343
10.1.9 NTP and Daylight Saving Time Parameters 344
10.2 Web and Telnet Parameters 345
10.2.1 General Parameters 345
10.2.2 Web Parameters 346
10.2.3 Telnet Parameters 348
10.3 Debugging and Diagnostics Parameters 348
10.3.1 General Parameters 348
10.3.2 Syslog, CDR and Debug Parameters 350
10.3.3 Remote Alarm Indication Parameters 353
10.3.4 Serial Parameters 353
10.3.5 BootP Parameters 354
10.4 Security Parameters 356
10.4.1 General Parameters 356
10.4.2 HTTPS Parameters 357
10.4.3 SRTP Parameters 358
10.4.4 TLS Parameters 360
10.4.5 SSH Parameters 361
10.4.6 IPSec Parameters 362
10.4.7 OCSP Parameters 364
10.5 RADIUS Parameters 364
10.6 SNMP Parameters 366
10.7 SIP Media Realm Parameters 369
10.8 Control Network Parameters 370
10.8.1 IP Group, Proxy, Registration and Authentication Parameters 370
10.9 General SIP Parameters 383
10.10 Coders and Profile Parameters 402
10.11 Channel Parameters 410
10.11.1 Voice Parameters 410
10.11.2 Coder Parameters 412
10.11.3 Fax and Modem Parameters 412
10.11.4 DTMF Parameters 417
10.11.5 RTP, RTCP and T.38 Parameters 418
10.12 Gateway and IP-to-IP Parameters 422
10.12.1 Fax and Modem Parameters 422
10.12.2 DTMF and Hook-Flash Parameters 424
10.12.3 Digit Collection and Dial Plan Parameters 429
10.12.4 Voice Mail Parameters 431
10.12.5 Supplementary Services Parameters 434
10.12.5.1 Caller ID Parameters 434
10.12.5.2 Call Waiting Parameters 439
10.12.5.3 Call Forwarding Parameters 442
10.12.5.4 Message Waiting Indication Parameters 444
10.12.5.5 Call Hold Parameters 446
10.12.5.6 Call Transfer Parameters 447
10.12.5.7 Three-Way Conferencing Parameters 448
10.12.5.8 Emergency Call Parameters 450
10.12.5.9 Call Cut-Through Parameters 451
10.12.5.10 Automatic Dialing Parameters 451
10.12.5.11 Direct Inward Dialing Parameters 452
10.12.5.12 MLPP Parameters 454
10.12.6 Answer and Disconnect Supervision Parameters 456
10.12.7 Tone Parameters 461
10.12.7.1 Telephony Tone Parameters 461
10.12.7.2 Tone Detection Parameters 464

10.12.7.3 Metering Tone Parameters 465
10.12.8 Telephone Keypad Sequence Parameters 467
10.12.9 General FXO Parameters 471
10.12.10 FXS Parameters 473
10.12.11 Hunt Groups, Number Manipulation and Routing Parameters 474
10.12.11.1 Hunt Groups and Routing Parameters 474
10.12.11.2 Alternative Routing Parameters 480
10.12.11.3 Number Manipulation Parameters 484
10.13 Standalone Survivability Parameters 492
10.14 Auxiliary and Configuration Files Parameters 496
10.14.1 Auxiliary/Configuration File Name Parameters 496
10.14.2 Automatic Update Parameters 497
11 SIP Software Package 499
12 Selected Technical Specifications 501

List of Figures

Figure 1-1: Typical MediaPack VoIP Application 22
Figure 3-1: Login Screen 29
Figure 3-2: Main Areas of the Web Interface GUI 30
Figure 3-3: "Reset" Displayed on Toolbar 31
Figure 3-4: Navigation Tree 32
Figure 3-5: Toggling between Basic and Full View 33
Figure 3-6: Showing and Hiding Navigation Pane 34
Figure 3-7: Toggling between Basic and Advanced View 36
Figure 3-8: Expanding and Collapsing Parameter Groups 37
Figure 3-9: Edit Symbol after Modifying Parameter Value 37
Figure 3-10: Value Reverts to Previous Valid Value 38
Figure 3-11: Adding an Index Entry to a Table 39
Figure 3-12: Compacting a Web Interface Table 40
Figure 3-13: Searched Result Screen 41
Figure 3-14: Scenario Creation Confirm Message Box 42
Figure 3-15: Creating a Scenario 43
Figure 3-16: Scenario Loading Message Box 44
Figure 3-17: Scenario Example 44
Figure 3-18: Scenario File Page 47
Figure 3-19: Scenario Loading Message Box 48
Figure 3-20: Message Box for Confirming Scenario Deletion 49
Figure 3-21: Confirmation Message Box for Exiting Scenario Mode 49
Figure 3-22: User-Defined Web Welcome Message after Login 50
Figure 3-23: Help Topic for Current Page 51
Figure 3-24: Log Off Confirmation Box 52
Figure 3-25: Web Session Logged Off 52
Figure 3-26: MP-11x Home Page 53
Figure 3-27: MP-124 Home Page 53
Figure 3-28: Shortcut Menu (e.g. MP-11x) 55
Figure 3-29: Typing Port Name (e.g. MP-11x) 55
Figure 3-30: Shortcut Menu (e.g. MP-11x) 55
Figure 3-31: Shortcut Menu (e.g. MP-11x) 56
Figure 3-32: Basic Channel Information Page 56
Figure 3-33: Application Settings Page 58
Figure 3-34: NFS Settings Page 59
Figure 3-35: Syslog Settings Page 61
Figure 3-36: Regional Settings Page 62
Figure 3-37: Certificates Signing Request Page 63
Figure 3-38: IKE Table Listing Loaded Certificate Files 64
Figure 3-39: WEB User Accounts Page (for Users with 'Security Administrator' Privileges) 68
Figure 3-40: WEB Security Settings Page 69
Figure 3-41: Telnet/SSH Settings Page 70
Figure 3-42: Web & Telnet Access List Page - Add New Entry 70
Figure 3-43: Web & Telnet Access List Table 71
Figure 3-44: RADIUS Parameters Page 72
Figure 3-45: SNMP Community String Page 73
Figure 3-46: SNMP Trap Destinations Page 74
Figure 3-47: SNMP Trusted Managers 75
Figure 3-48: SNMP V3 Setting Page 76
Figure 3-49: IP Settings Page 79
Figure 3-50: Confirmation Message for Accessing the Multiple Interface Table 80
Figure 3-51: IP Routing Table Page 83
Figure 3-52: QoS Settings Page 85
Figure 3-53: DNS Settings Page 86
Figure 3-54: Internal DNS Table Page 87
Figure 3-55: Internal SRV Table Page 88

Figure 3-56: Firewall Settings Page 90
Figure 3-57: 8021x Settings Page 93
Figure 3-58: General Security Settings Page 93
Figure 3-59: IP Security Proposals Table 94
Figure 3-60: IP Security Associations Table Page 95
Figure 3-61: Voice Settings Page 98
Figure 3-62: Fax/Modem/CID Settings Page 99
Figure 3-63: RTP/RTCP Settings Page 100
Figure 3-64: General Media Settings Page 101
Figure 3-65: Analog Settings Page 101
Figure 3-66: Media Security Page 102
Figure 3-67: Applications Enabling Page 103
Figure 3-68: IP Group Table Page 104
Figure 3-69: Proxy Sets Table Page 106
Figure 3-70: SIP General Parameters Page 111
Figure 3-71: Advanced Parameters Page 112
Figure 3-72: Account Table Page 113
Figure 3-73: Proxy & Registration Page 116
Figure 3-74: RADIUS Parameters Page 117
Figure 3-75: Coders Page 118
Figure 3-76: Coder Group Settings Page 120
Figure 3-77: Tel Profile Settings Page 121
Figure 3-78: IP Profile Settings Page 123
Figure 3-79: Endpoint Phone Number Table Page 125
Figure 3-80: Hunt Group Settings Page 126
Figure 3-81: General Settings Page 129
Figure 3-82: Source Phone Number Manipulation Table for Tel-to-IP Calls 131
Figure 3-83: Redirect Number Tel to IP Page 134
Figure 3-84: Phone Context Table Page 135
Figure 3-85: Routing General Parameters Page 137
Figure 3-86: Tel to IP Routing Page 139
Figure 3-87: Inbound IP Routing Table Page 142
Figure 3-88: Reasons for Alternative Routing Page 145
Figure 3-89: Forward on Busy Trunk Destination Page 146
Figure 3-90: DTMF & Dialing Page 147
Figure 3-91: Supplementary Services Page 148
Figure 3-92: Keypad Features Page 150
Figure 3-93: Metering Tones Page 151
Figure 3-94: Charge Codes Table Page 152
Figure 3-95: FXO Settings Page 153
Figure 3-96: Automatic Dialing Page 155
Figure 3-97: Caller Display Information Page 156
Figure 3-98: Call Forward Table Page 157
Figure 3-99: Caller ID Permissions Page 158
Figure 3-100: Call Waiting Page 159
Figure 3-101: Voice Mail Settings Page 160
Figure 3-102: SAS Configuration Page 162
Figure 3-103: Maintenance Actions Page 166
Figure 3-104: Reset Confirmation Message Box 167
Figure 3-105: Device Lock Confirmation Message Box 168
Figure 3-106: Load Auxiliary Files Page 171
Figure 3-107: Software Upgrade Key Status Page 173
Figure 3-108: Software Upgrade Key with Multiple S/N Lines 174
Figure 3-109: Start Software Upgrade Wizard Screen 176
Figure 3-110: End Process Wizard Page 178
Figure 3-111: Configuration File Page 179
Figure 3-112: Message Log Page 181
Figure 3-113: Device Information Page 182
Figure 3-114: Ethernet Port Information Page 183

Figure 3-115: IP Interface Status Page 184
Figure 3-116: Basic Statistics Page 184
Figure 3-117: Calls Count Page 185
Figure 3-118: SAS/SBC Registered Users Page 187
Figure 3-119: Call Routing Status Page 188
Figure 3-120: Registration Status Page 189
Figure 3-121: IP Connectivity Page 190
Figure 5-1: Areas of the EMS GUI 199
Figure 5-2: EMS Login Screen 202
Figure 5-3: Adding a Region 203
Figure 5-4: Defining the IP Address 203
Figure 5-5: SIP Protocol Definitions Frame 204
Figure 5-6: IPSec Table Screen 205
Figure 5-7: Authentication & Security Screen 206
Figure 5-8: MG Information Screen 209
Figure 5-9: SNMP Configuration Screen 210
Figure 5-10: Confirmation for Saving Configuration and Resetting Device 211
Figure 5-11: Software Manager Screen 212
Figure 5-12: Add Files Screen 212
Figure 5-13: Files Manager Screen 213
Figure 6-1: RestoreFactorySettings CLI Command 215
Figure 7-1: Example of a User Information File 225
Figure 8-1: Prefix to Add Field with Notation 232
Figure 8-2: Call Flow for One-Stage Dialing 235
Figure 8-3: Call Flow for Two-Stage Dialing 236
Figure 8-4: Call Flow for Automatic Dialing 238
Figure 8-5: Call Flow for Collecting Digits 239
Figure 8-6: FXO-FXS Remote PBX Extension (Example) 242
Figure 8-7: MWI for Remote Extensions 244
Figure 8-8: Call Waiting for Remote Extensions 244
Figure 8-9: Assigning Phone Numbers to FXS Endpoints 244
Figure 8-10: Automatic Dialing for FXS Ports 245
Figure 8-11: 1. FXS Tel-to-IP Routing Configuration 245
Figure 8-12: Assigning Phone Numbers to FXO Ports 245
Figure 8-13: FXO Automatic Dialing Configuration 246
Figure 8-14: FXO Tel-to-IP Routing Configuration 246
Figure 8-15: Double Hold SIP Call Flow 256
Figure 8-16: Call Forward Reminder with Application Server 260
Figure 8-17: SIP Call Flow 268
Figure 8-18: Assigning Phone Numbers to Device 10.2.37.10 274
Figure 8-19: Assigning Phone Numbers to Device 10.2.37.20 274
Figure 8-20: Routing Calls Between Devices 274
Figure 8-21: Routing Between ITSPs and Enterprise (Example) 275
Figure 8-22: Configuring Proxy Set ID #1 in the Proxy Sets Table Page 276
Figure 8-23: Configuring IP Groups #1 and #2 in the IP Group Table Page 276
Figure 8-24: Assigning Channels to Hunt Groups 277
Figure 8-25: Configuring Registration Mode for Hunt Groups and Assigning to IP Group 277
Figure 8-26: Configuring Username and Password for Channels 5-8 in Authentication Page 277
Figure 8-27: Configuring Account for Registration to ITSP 1 277
Figure 8-28: Configuring ITSP-to-Hunt Group Routing 278
Figure 8-29: Configuring Hunt Group to ITSP Routing 278
Figure 8-30: SAS Outbound Mode in Normal State (Example) 280
Figure 8-31: SAS Outbound Mode in Emergency State (Example) 281
Figure 8-32: SAS Redundant Mode in Normal State (Example) 282
Figure 8-33: SAS Redundant Mode in Emergency State (Example) 283
Figure 8-34: Flowchart of INVITE from UA's in SAS Normal State 284
Figure 8-35: Flowchart of INVITE from Primary Proxy in SAS Normal State 285
Figure 8-36: Flowchart for SAS Emergency State 286

Figure 8-37: Enabling the SAS Application 287
Figure 8-38: Configuring Common Settings 289
Figure 8-39: Defining UAs' Proxy Server 290
Figure 8-40: Enabling Proxy Server for Gateway Application 292
Figure 8-41: Defining Proxy Server for Gateway Application 292
Figure 8-42: Disabling user=phone in SIP URL 293
Figure 8-43: Enabling Proxy Server for Gateway Application 293
Figure 8-44: Defining Proxy Servers for Gateway Application 294
Figure 8-45: Disabling user=phone in SIP URL 294
Figure 8-46: Manipulating User Part in Incoming REGISTER 296
Figure 8-47: Manipulating INVITE Destination Number 297
Figure 8-48: Blocking Unregistered SAS Users 298
Figure 8-49: Configuring SAS Emergency Numbers 299
Figure 9-1: Nat Functioning 312
Figure 9-2: Multiple Network Interfaces 316
Figure 9-3: Interface Column 326

List of Tables

Table 1-1: Supported MediaPack Series Configurations 21
Table 3-1: Description of Toolbar Buttons....31
Table 3-2: ini File Parameter for Welcome Login Message 50
Table 3-3: Description of the Areas of the Home Page....54
Table 3-4: NFS Settings Parameters 60
Table 3-5: Web User Accounts Access Levels and Privileges....67
Table 3-6: Default Attributes for the Web User Accounts 67
Table 3-7: SNMP Community String Parameters Description 74
Table 3-8: SNMP Trap Destinations Parameters Description....74
Table 3-9: SNMP V3 Users Parameters 76
Table 3-10: Multiple Interface Table Parameters Description 80
Table 3-11: IP Routing Table Description 83
Table 3-12: Internal Firewall Parameters 91
Table 3-13: IP Security Proposals Table Configuration Parameters 94
Table 3-14: Default IPSec/IKE Proposals 95
Table 3-15: IP Security Associations Table Configuration Parameters 96
Table 3-16: IP Group Parameters 104
Table 3-17: Proxy Sets Table Parameters 107
Table 3-18: Account Table Parameters Description 114
Table 3-19: Endpoint Phone Number Table Parameters 125
Table 3-20: Hunt Group Settings Parameters....127
Table 3-21: Number Manipulation Parameters Description 132
Table 3-22: Redirect Number Tel to IP Parameters Description....134
Table 3-23: Phone-Context Parameters Description 136
Table 3-24: Tel-to-IP Routing Table Parameters 140
Table 3-25: IP-to-Tel Routing Table Description....143
Table 3-26: Call Forward Table....157
Table 3-27: SAS IP2IP Routing Table Parameters 163
Table 3-28: Auxiliary Files Descriptions 170
Table 3-29: Ethernet Port Information Parameters 183
Table 3-30: Call Counters Description 185
Table 3-31: SAS/SBC Registered Users Parameters 187
Table 3-32: Call Routing Status Parameters....188
Table 3-33: IP Connectivity Parameters....190
Table 7-1: User Information Items....224
Table 8-1: Dialing Plan Notations....228
Table 8-2: Digit Map Pattern Notations 229
Table 8-3: MLPP Call Priority Levels (Precedence) and DSCP Configuration Parameters 266
Table 8-4: Supported X-Detect Event Types....301
Table 8-5: Special Information Tones (SITs) Reported by the device 302
Table 8-6: Supported RADIUS Attributes....304
Table 8-7: Supported CDR Fields 306
Table 9-1: Multiple Interface Table....317
Table 9-2: Application Types....318
Table 9-3: Configured Default Gateway Example....319
Table 9-4: Separate Routing Table Example 319
Table 9-5: Quality of Service Parameters 321
Table 9-6: Traffic/Network Types and Priority 322
Table 9-7: Application Type Parameters....323
Table 9-8: IP Routing Table Layout....325
Table 9-9: Multiple Interface Table - Example 1 329
Table 9-10: Routing Table - Example 1....329
Table 9-11: Multiple Interface Table - Example2....330
Table 9-12: Routing Table - Example 2....330
Table 9-13: Multiple Interface Table - Example 3....331
Table 9-14: Routing Table - Example 3....331

Table 10-1: Ethernet Parameters 333
Table 10-2: IP Network Interfaces and VLAN Parameters....334
Table 10-3: Static Routing Parameters 337
Table 10-4: QoS Parameters 338
Table 10-5: NAT and STUN Parameters....339
Table 10-6: NFS Parameters 341
Table 10-7: DNS Parameters 342
Table 10-8: DHCP Parameters 343
Table 10-9: NTP and Daylight Saving Time Parameters 344
Table 10-10: General Web and Telnet Parameters 345
Table 10-11: Web Parameters 346
Table 10-12: Telnet Parameters....348
Table 10-13: General Debugging and Diagnostic Parameters 348
Table 10-14: Syslog, CDR and Debug Parameters 350
Table 10-15: RAI Parameters....353
Table 10-16: Serial Parameters 353
Table 10-17: BootP Parameters....354
Table 10-18: General Security Parameters....356
Table 10-19: HTTPS Parameters....357
Table 10-20: SRTP Parameters 358
Table 10-21: TLS Parameters 360
Table 10-22: SSH Parameters 361
Table 10-23: IPSec Parameters 362
Table 10-24: OCSP Parameters 364
Table 10-25: RADIUS Parameters 364
Table 10-26: SNMP Parameters 366
Table 10-27: SIP Media Realm Parameters....369
Table 10-28: Proxy, Registration and Authentication SIP Parameters 370
Table 10-29: General SIP Parameters 383
Table 10-30: Profile Parameters 402
Table 10-31: Voice Parameters....410
Table 10-32: Coder Parameters....412
Table 10-33: Fax and Modem Parameters....412
Table 10-34: DTMF Parameters....417
Table 10-35: RTP/RTCP and T.38 Parameters 418
Table 10-36: Fax and Modem Parameters....422
Table 10-37: DTMF and Hook-Flash Parameters 424
Table 10-38: Digit Collection and Dial Plan Parameters 429
Table 10-39: Voice Mail Parameters 431
Table 10-40: Caller ID Parameters....434
Table 10-41: Call Waiting Parameters 439
Table 10-42: Call Forwarding Parameters 442
Table 10-43: MWI Parameters 444
Table 10-44: Call Hold Parameters 446
Table 10-45: Call Transfer Parameters 447
Table 10-46: Three-Way Conferencing Parameters 448
Table 10-47: Emergency Call Parameters 450
Table 10-48: Call Cut-Through Parameters 451
Table 10-49: Automatic Dialing Parameters....451
Table 10-50: DID Parameters 452
Table 10-51: MLPP Parameters....454
Table 10-52: Answer and Disconnect Parameters....456
Table 10-53: Tone Parameters 461
Table 10-54: Tone Detection Parameters 464
Table 10-55: Metering Tone Parameters 465
Table 10-56: Keypad Sequence Parameters 467
Table 10-57: General FXO Parameters 471
Table 10-58: General FXS Parameters....473
Table 10-59: Routing Parameters 474

Table 10-60: Alternative Routing Parameters 480
Table 10-61: Number Manipulation Parameters 484
Table 10-62: SAS Parameters 492
Table 10-63: Auxiliary and Configuration File Parameters.....496
Table 10-64: Automatic Update of Software and Configuration Files Parameters 497
Table 11-1: Software Package 499
Table 12-1: MediaPack Technical Specifications.....501

Reader's Notes

Notice

This document describes the AudioCodes MediaPack series MP-11x and MP-124 Voice over IP (VoIP) gateways.

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 2011 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: February-13-2011

Trademarks

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

WEEE EU Directive

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

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com.

Abbreviations and Terminology

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

Regulatory Information

The Regulatory Information can be viewed at http://www.audiocodes.com/downloads.

Related Documentation

Manual Name
SIP CPE Release Notes
Product Reference Manual for SIP CPE Devices
MP-11x & MP-124 SIP Installation Manual
MP-11x SIP Fast Track Guide
MP-124 AC SIP Fast Track Guide
MP-124 DC SIP Fast Track Guide
CPE Configuration Guide for IP Voice Mail

Warning: The device is supplied as a sealed unit and must only be serviced by qualified service personnel.

Note: Throughout this manual, unless otherwise specified, the following naming conventions are used :

- The term *device* refers to the MediaPack series gateways.
- The term *MediaPack* refers to the MP-124, MP-118, MP-114, and MP-112 VoIP devices.
- The term *MP-11x* refers to the MP-118, MP-114, and MP-112 VoIP devices.

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

Note: For assigning an IP address to the device for initial connectivity, refer to the *Installation Manual*.

Note: 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 the PSTN/PBX and destined for the IP network.

Notes:

- 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.

Reader's Notes

1 Overview

This manual provides you with information for configuring and operating the VoIP analog MediaPack series devices listed in the table below:

Table 1-1: Supported MediaPack Series Configurations

Product Name	FXS	FXO	Combined FXS/FXO	Number of Channels
MP-124	✓	×	×	24
MP-118	✓	✓	4 + 4	8
MP-114	✓	✓	2 + 2	4
MP-112*	✓	×	×	2

* The MP-112 differs from the MP-114 and MP-118 in that its configuration excludes the RS-232 connector, Lifeline option, and outdoor protection.

1.1 Gateway Description

The MediaPack series analog Voice-over-IP (VoIP) Session Initiation Protocol (SIP) media gateways (hereafter referred to as *device*) are cost-effective, cutting edge technology products. These stand-alone analog VoIP devices provide superior voice technology for connecting legacy telephones, fax machines and Private Branch Exchange (PBX) systems to IP-based telephony networks, as well as for integration with new IP-based PBX architectures. These devices are designed and tested to be fully interoperable with leading softswitches and SIP servers.

The device is best suited for small and medium-sized enterprises (SME), branch offices, or residential media gateway solutions. The device enables users to make local or international telephone and / or fax calls over the Internet between distributed company offices, using their existing telephones and fax. These calls are routed over the existing network ensuring that voice traffic uses minimum bandwidth. The device also provides SIP trunking capabilities for Enterprises operating with multiple Internet Telephony Service Providers (ITSP) for VoIP services.

The device supports the SIP protocol, enabling the deployment of VoIP solutions in environments where each enterprise or residential location is provided with a simple media gateway. This provides the enterprise with a telephone connection (i.e., RJ-11 connector) and the capability to transmit voice and telephony signals over a packet network.

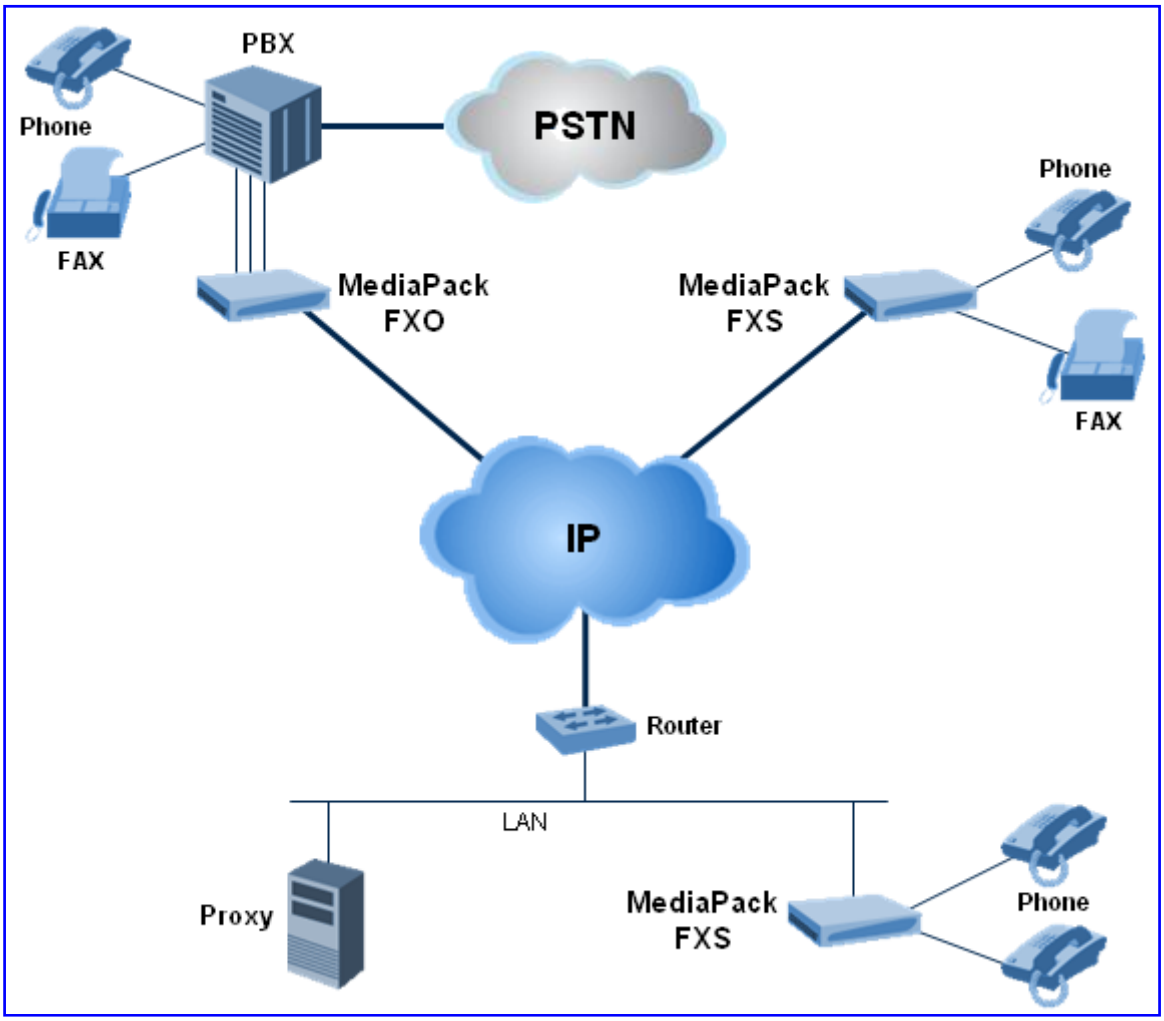
The device provides FXO and/or FXS analog ports for direct connection to an enterprise's PBX (FXO), and / or to phones, fax machines, and modems (FXS). Depending on model, the device can support up to 24 simultaneous VoIP calls. The device is also equipped with a 10/100Base-TX Ethernet port for connection to the IP network. The device provides LEDs for indicating operating status of the various interfaces.

The device is a compact unit that can be easily mounted on a desktop, wall, or in a 19-inch rack.

The device provides a variety of management and provisioning tools, including an HTTP-based embedded Web server, Telnet, Element Management System (EMS), and Simple Network Management Protocol (SNMP). The user-friendly, Web interface provides remote configuration using any standard Web browser (such as Microsoft™ Internet Explorer™).

The figure below illustrates a typical MediaPack VoIP application.

Figure 1-1: Typical MediaPack VoIP Application



1.2 MediaPack Features

This section provides a high-level overview of some of the many device supported features. For more updated information on the device's supported features, refer to the latest MP-11x & MP-124 SIP Release Notes.

1.2.1 MP-11x Hardware Features

The MP-11x series hardware features includes the following:

- Combined FXS / FXO devices (four FXS and four FXO ports on the MP-118; two FXS and two FXO ports on the MP-114).
- MP-11x compact, rugged enclosure -- only one-half of a 19-inch rack unit, 1 U high.
- Lifeline - provides a wired phone connection to the PSTN line that becomes active upon a power or network failure (combined FXS/FXO devices provide a Lifeline connection that's available on all FXS ports).
- LEDs on the front panel that provide information on the device's operating status and the network interface.
- Reset button on the rear panel for restarting the MP-11x and for restoring the MP-11x parameters to their factory default settings.

1.2.2 MP-124 Hardware Features

The MP-124 hardware features include the following:

- MP-124 19-inch, 1U rugged enclosure provides up to 24 analog FXS ports, using a single 50-pin Telco connector.
- LEDs on the front panel that provide information on the device's operating status and the network interface.
- Reset button on the front panel for restarting the MP-124 and for restoring the MP-124 parameters to their factory default settings.

1.3 SIP Overview

Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol used on the gateway for creating, modifying, and terminating sessions with one or more participants. These sessions can include Internet telephone calls, media announcements, and conferences.

SIP invitations are used to create sessions and carry session descriptions that enable participants to agree on a set of compatible media types. SIP uses elements called Proxy servers to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies and provide features to users.

SIP also provides a registration function that enables users to upload their current locations for use by Proxy servers. SIP implemented in the gateway, complies with the Internet Engineering Task Force (IETF) RFC 3261 (refer to http://www.ietf.org).

2 Configuration Tools

You can configure the device, using the following management tools:

- The device's HTTP-based Embedded Web Server (Web interface), using any standard Web browser (described in "Web-based Management" on page 27).
- A configuration *ini* file loaded to the device (see "ini File Configuration" on page 193).
- AudioCodes' Element Management System (see "Element Management System (EMS)" on page 199).
- Simple Network Management Protocol (SNMP) browser software (refer to the *Product Reference Manual*).

Note: To initialize the device by assigning it an IP address, a firmware file (cmp), and a configuration file (ini file), you can use AudioCodes' BootP/TFTP utility, which accesses the device using the device's MAC address (refer to the Product Reference Manual).

Reader's Notes

3 Web-Based Management

The device's Embedded Web Server (*Web interface*) provides FCAPS (fault management, configuration, accounting, performance, and security) functionality. The Web interface allows you to remotely configure your device for quick-and-easy deployment, including uploading of software (*.cmp), configuration (*.ini), and auxiliary files, and resetting the device. The Web interface provides real-time, online monitoring of the device, including display of alarms and their severity. In addition, it displays performance statistics of voice calls and various traffic parameters.

The Web interface provides a user-friendly, graphical user interface (GUI), which can be accessed using any standard Web browser (e.g., Microsoft™ Internet Explorer). Access to the Web interface is controlled by various security mechanisms such as login user name and password, read-write privileges, and limiting access to specific IP addresses.

Notes:

- For a detailed description of all the parameters in the Web interface, see "Configuration Parameters Reference" on page 333.
- The parameters in the Web interface can alternatively be configured using their corresponding *ini* file parameters, which are enclosed in square brackets "[...]" in "Configuration Parameters Reference" on page 333.
- The Web interface allows you to configure most of the device's settings. However, additional configuration parameters may exist that are not provided in the Web interface and which can only be configured using *ini* file parameters. These parameters are listed without a corresponding Web parameter name in "Configuration Parameters Reference" on page 333.
- Some Web interface pages are Software Upgrade Key dependant. These pages appear only if the installed Software Upgrade Key supports the features related to the pages. For viewing your Software Upgrade Key, see "Loading Software Upgrade Key" on page 172.

3.1 Getting Acquainted with the Web Interface

This section describes the Web interface with regards to its graphical user interface (GUI) and basic functionality.

3.1.1 Computer Requirements

To use the device's Web interface, the following is required:

- A connection to the Internet network (World Wide Web).
- A network connection to the device's Web interface.
- One of the following Web browsers:
  - Microsoft™ Internet Explorer™ (version 6.0 or later)
  - Mozilla Firefox® (version 2.5 or later)
- Recommended screen resolutions: 1024 x 768 pixels, or 1280 x 1024 pixels.

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

3.1.2 Accessing the Web Interface

The Web interface can be opened using any standard Web browser (see "Computer Requirements" on page 28). When you initially access the Web interface, use the default user name ('Admin') and password ('Admin'). For changing the login user name and password, see "Configuring the Web User Accounts" on page 66).

Note: For assigning an IP address to the device, refer to the *Installation Manual*.

➢ **To access the Web interface:**

1. Open a standard Web browser application.
2. In the Web browser's Uniform Resource Locator (URL) field, specify the device's IP address (e.g., http://10.1.10.10); the Web interface's Login screen appears, as shown in the figure below**:**

Figure 3-1: Login Screen

3. In the 'User Name' and 'Password' fields, enter the case-sensitive, user name and password.
4. Click the **OK** button; the Web interface is accessed, displaying the 'Home' page (for a detailed description of the 'Home' page, see "Using the Home Page" on page 53).

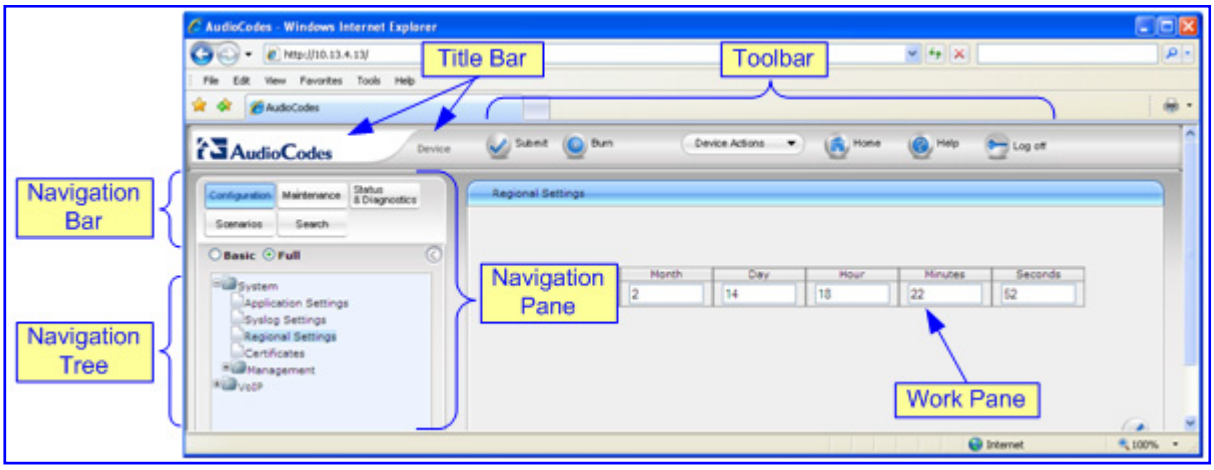
Note: If access to the device's Web interface is denied ("Unauthorized") due to Microsoft Internet Explorer security settings, perform the following:

1. Delete all cookies in the Temporary Internet Files folder. If this does not resolve the problem, the security settings may need to be altered (continue with Step 2).
2. In Internet Explorer, navigate to **Tools** menu > **Internet Options** > **Security** tab > **Custom Level**, and then scroll down to the Logon options and select **Prompt for username and password**. Select the **Advanced** tab, and then scroll down until the HTTP 1.1 Settings are displayed and verify that **Use HTTP 1.1** is selected.
3. Quit and start the Web browser again.

3.1.3 Areas of the GUI

The figure below displays the general layout of the Graphical User Interface (GUI) of the Web interface:

Figure 3-2: Main Areas of the Web Interface GUI



The Web GUI is composed of the following main areas:

- **Title bar:** Displays the corporate logo and product name.
- **Toolbar:** Provides frequently required command buttons for configuration (see "Toolbar" on page 31).
- **Navigation Pane:** Consists of the following areas:
  - **Navigation bar:** Provides tabs for accessing the configuration menus (see "Navigation Tree" on page 32), creating a Scenario (see Scenarios on page 41), and searching *ini* file parameters that have corresponding Web interface parameters (see "Searching for Configuration Parameters" on page 40).
  - **Navigation tree:** Displays the elements pertaining to the tab selected on the Navigation bar (tree-like structure of the configuration menus, Scenario Steps, or Search engine).
- **Work pane:** Displays configuration pages where configuration is performed (see "Working with Configuration Pages" on page 35).

3.1.4 Toolbar

The toolbar provides command buttons for quick-and-easy access to frequently required commands, as described in the table below:

Table 3-1: Description of Toolbar Buttons

Icon	Button Name	Description
	Submit	Applies parameter settings to the device (see "Saving Configuration" on page 169). **Note:** This icon is grayed out when not applicable to the currently opened page.
	Burn	Saves parameter settings to flash memory (see "Saving Configuration" on page 169).
	Device Actions	Opens a drop-down menu list with frequently needed commands: ▪ **Load Configuration File:** opens the 'Configuration File' page for loading an *ini* file (see "Backing Up and Loading Configuration File" on page 178). ▪ **Save Configuration File:** opens the 'Configuration File' page for saving the *ini* file to a PC (see "Backing Up and Loading Configuration File" on page 178). ▪ **Reset:** opens the 'Maintenance Actions' page for resetting the device (see "Resetting the Device" on page 167). ▪ **Software Upgrade Wizard:** opens the 'Software Upgrade Wizard' page for upgrading the device's software (see "Software Upgrade Wizard" on page 175).
	Home	Opens the 'Home' page (see "Using the Home Page" on page 53).
	Help	Opens the Online Help topic of the currently opened configuration page in the Work pane (see "Getting Help" on page 51).
	Log off	Logs off a session with the Web interface (see "Logging Off the Web Interface" on page 52).

Note: If you modify parameters that take effect only after a device reset, after you click the **Submit** button, the toolbar displays the word "Reset" (in red color), as shown in the figure below. This is a reminder to later save ('burn') your settings to flash memory and reset the device.

Figure 3-3: "Reset" Displayed on Toolbar

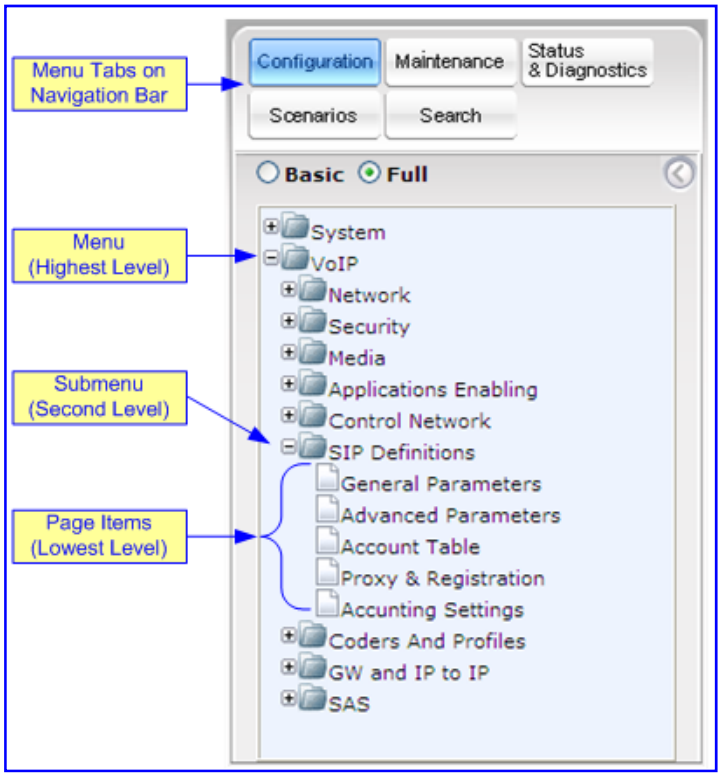
3.1.5 Navigation Tree

The Navigation tree, located in the Navigation pane, displays the menus (pertaining to the menu tab selected on the Navigation bar) used for accessing the configuration pages. The Navigation tree displays a tree-like structure of menus. You can easily 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 3-4: Navigation Tree



➢ To view menus in the Navigation tree:

- On the Navigation bar, select the required tab:
  - **Configuration** (see "Configuration Tab" on page 57)
  - **Maintenance** (see "Maintenance Tab" on page 166)
  - **Status & Diagnostics** (see "Status & Diagnostics Tab" on page 180)

➢ To navigate to a page:

1. Navigate to the required page item, by performing the following:
   - Drilling-down using the **plus** signs to expand the menus and submenus
   - Drilling-up using the **minus** signs to collapse the menus and submenus
2. Select the required page item; the page opens in the Work pane.

3.1.5.1 Displaying Navigation Tree in Basic and Full View

You can view an expanded or reduced Navigation tree display regarding the number of listed menus and submenus. This is relevant when using the configuration tabs (**Configuration**, **Maintenance**, and **Status & Diagnostics**) on the Navigation bar.

The Navigation tree menu can be displayed in one of two views:

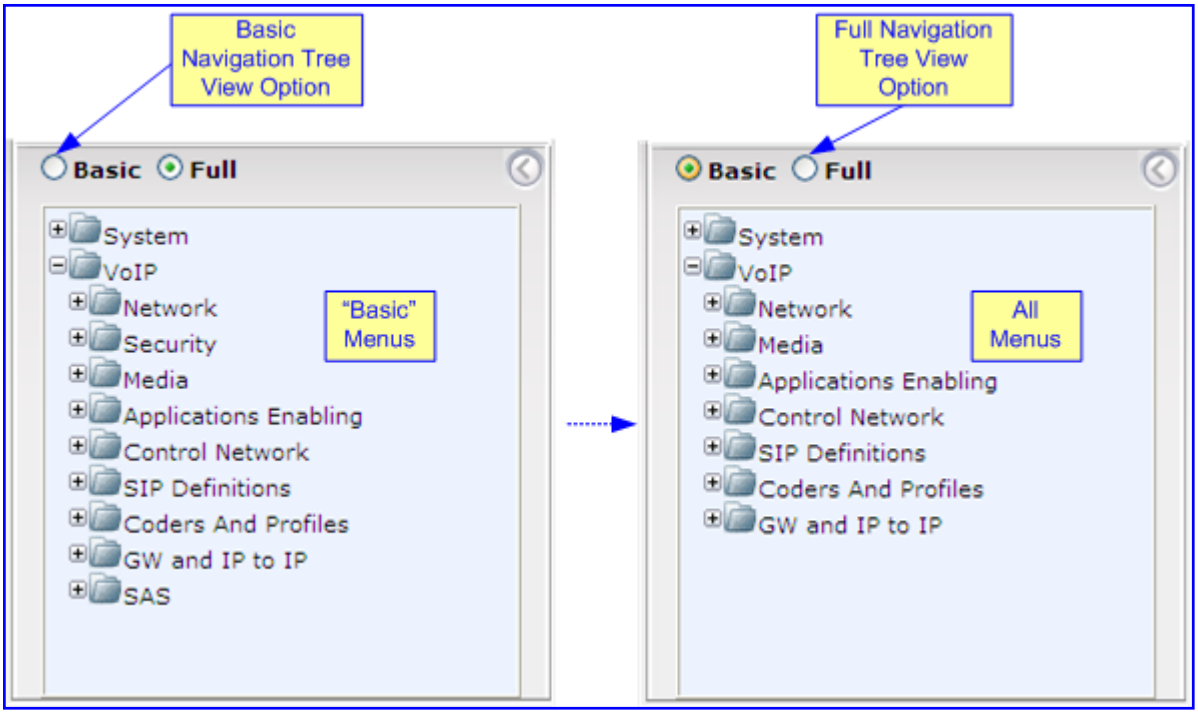
- **Basic:** displays only commonly used menus
- **Full:** displays all the menus pertaining to a configuration tab.

The advantage of the Basic view is that it prevents "cluttering" the Navigation tree with menus that may not be required. Therefore, a Basic view allows you to easily locate required menus.

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

- Select the **Basic** option (located below the Navigation bar) to display a reduced menu tree; select the **Full** option to display all the menus. By default, the **Basic** option is selected.

Figure 3-5: Toggling between Basic and Full View



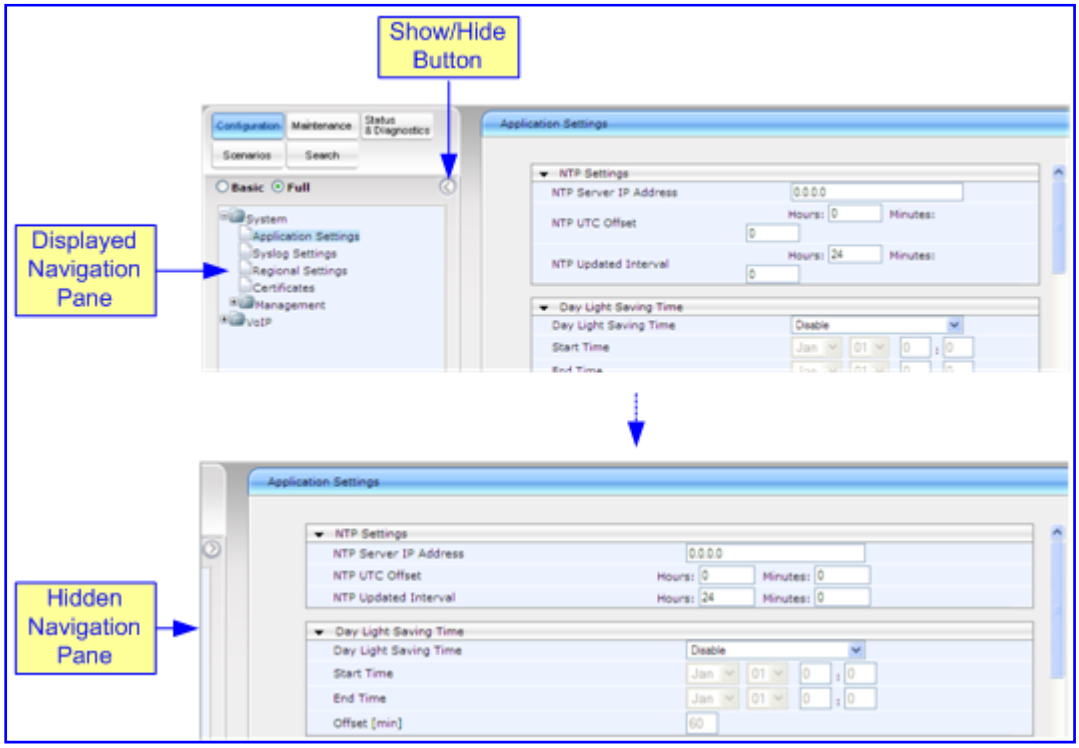
Note: When in Scenario mode (see Scenarios on page 41), the Navigation tree is displayed in 'Full' view (i.e., all menus are displayed in the Navigation tree).

3.1.5.2 Showing / Hiding the Navigation Pane

The Navigation pane can be hidden to provide more space for elements displayed in the Work pane. This is especially useful when the Work pane displays a page with a table that's wider than the Work pane and to view the all the columns, you need to use scroll bars. The arrow button located just below the Navigation bar is used 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 3-6: Showing and Hiding Navigation Pane



3.1.6 Working with Configuration Pages

The configuration pages contain the parameters for configuring the device. The configuration pages are displayed in the Work pane, which is located to the right of the Navigation pane.

3.1.6.1 Accessing Pages

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

➢ **To open a configuration page in the Work pane:**

1. On the Navigation bar, click the required tab:
   - **Configuration** (see "Configuration Tab" on page 57)
   - **Maintenance** (see "Maintenance Tab" on page 166)
   - **Status & Diagnostics** (see "Status & Diagnostics Tab" on page 180)

   The menus of the selected tab appear in the Navigation tree.
2. In the Navigation tree, drill-down to the required page item; the page opens in the Work pane.

You can also access previously opened pages, by clicking your 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" on page 31).
- To view all the menus in the Navigation tree, ensure that the Navigation tree is in 'Full' view (see "Displaying Navigation Tree in Basic and Full View" on page 33).
- To get Online Help for the currently displayed page, see "Getting Help" on page 51.
- Certain pages may not be accessible or may be read-only if your Web user account's access level is low (see "Configuring the Web User Accounts" on page 66). If a page is read-only, 'Read-Only Mode' is displayed at the bottom of the page.

3.1.6.2 Viewing Parameters

For convenience, some pages allow you to view a reduced or expanded display of parameters. A reduced display allows you to easily identify required parameters, enabling you to quickly configure your device.

The Web interface provides you with two methods for handling the display of page parameters:

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

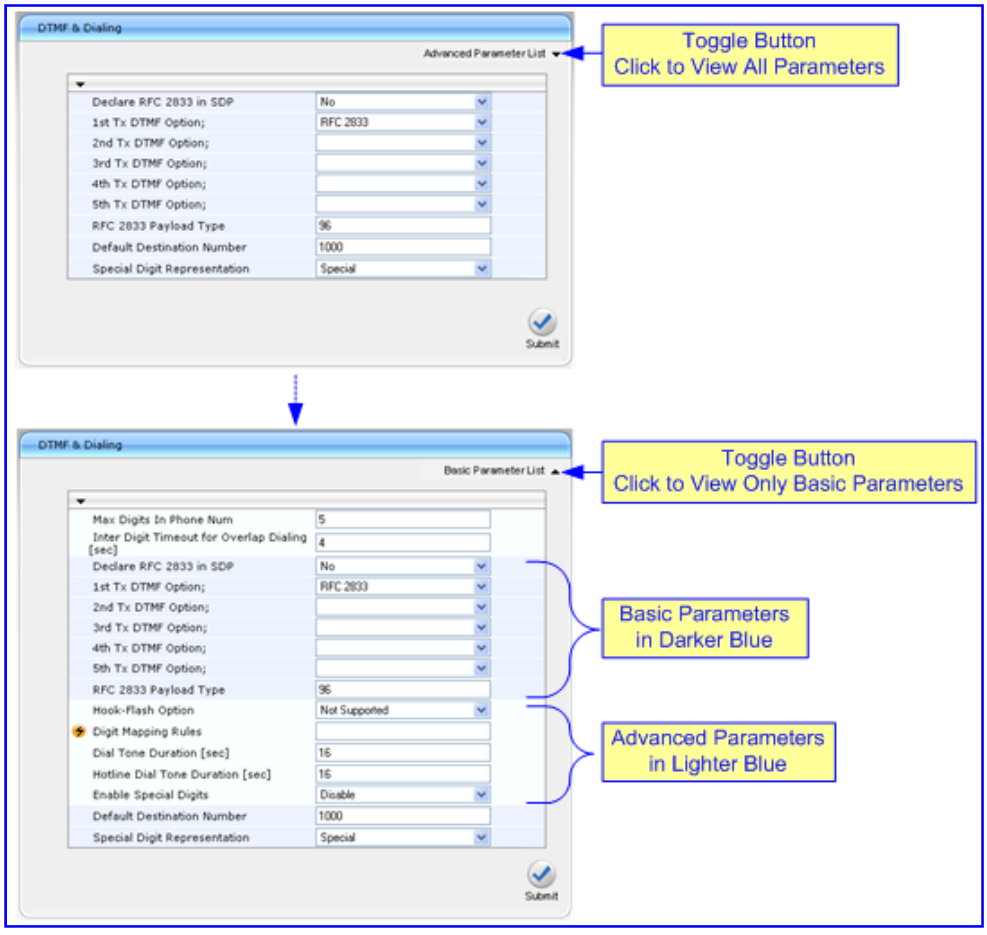
3.1.6.2.1 Displaying Basic and Advanced Parameters

Some pages provide you with an **Advanced Parameter List** / **Basic Parameter List** toggle button that allows you to show or hide advanced parameters (in addition to displaying the basic parameters). This button is located on the top-right corner of the page and has two 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, and then showing advanced parameters as well, using the **Advanced Parameter List** button.

Figure 3-7: Toggling between Basic and Advanced View



For ease of identification, the basic parameters are displayed with a darker blue color background than the advanced parameters.

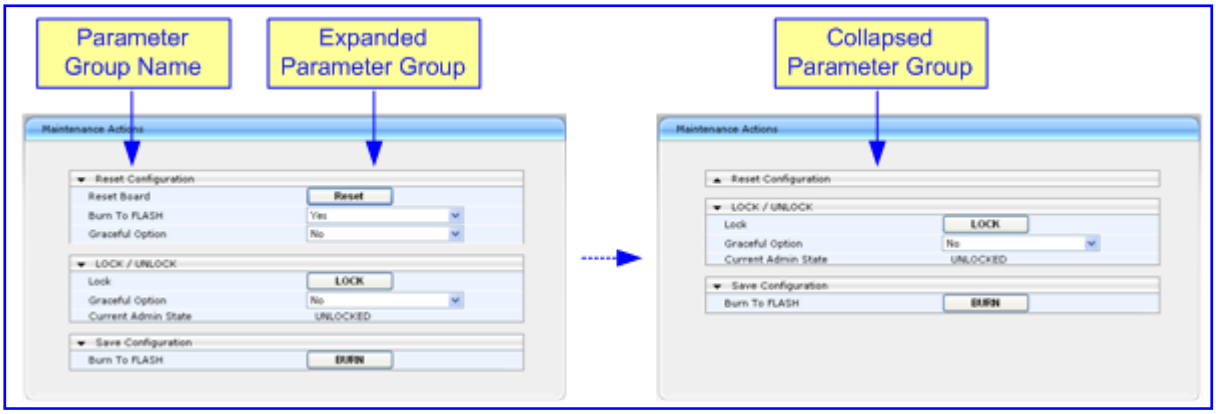
Notes:

- When the Navigation tree is in 'Full' mode (see "Navigation Tree" on page 32), configuration pages display all their parameters (i.e., the 'Advanced Parameter List' view is displayed).
- If a page contains only basic parameters, the **Basic Parameter List** button is not displayed.

3.1.6.2.2 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 name 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.

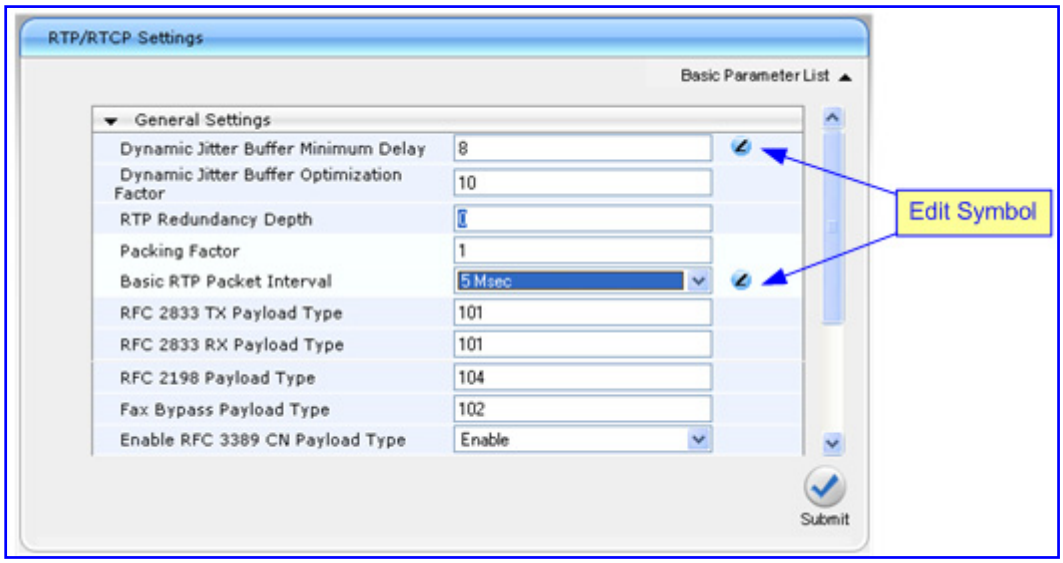
Figure 3-8: Expanding and Collapsing Parameter Groups



3.1.6.3 Modifying and Saving Parameters

When you change parameter values on a page, the **Edit** symbol appears to the right of these parameters. This is especially useful for indicating the parameters that you have currently modified (before applying the changes). After you save your parameter modifications (refer to the procedure described below), the **Edit** symbols disappear.

Figure 3-9: Edit Symbol after Modifying Parameter Value



➢ **To save configuration changes on a page to the device's volatile memory (RAM):**

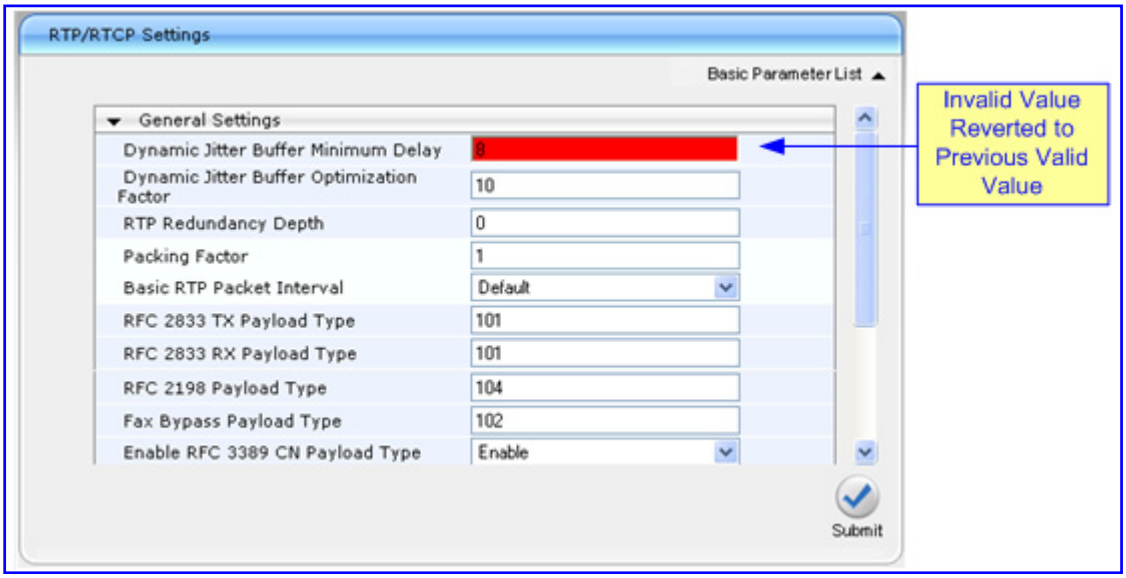
- Click the **Submit** button, which is located near the bottom of the page in which you are working; modifications to parameters with on-the-fly capabilities are immediately applied to the device and take effect; other parameters (displayed on the page with the lightning symbol) are not changeable on-the-fly and require a device reset (see "Resetting the Device" on page 167) before taking effect.

Notes:

- 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, you need to save ('burn') them to the device's non-volatile memory, i.e., flash (see "Saving Configuration" on page 169).
- If you modify a parameter value and then attempt to navigate away from the page without clicking **Submit**, a message box appears notifying you of this. Click **Yes** to save your modifications or **No** to ignore them.

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 3-10: Value Reverts to Previous Valid Value



3.1.6.4 Entering Phone Numbers

Phone numbers or prefixes that you need to configure throughout the Web interface must be entered 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.

3.1.6.5 Working with Tables

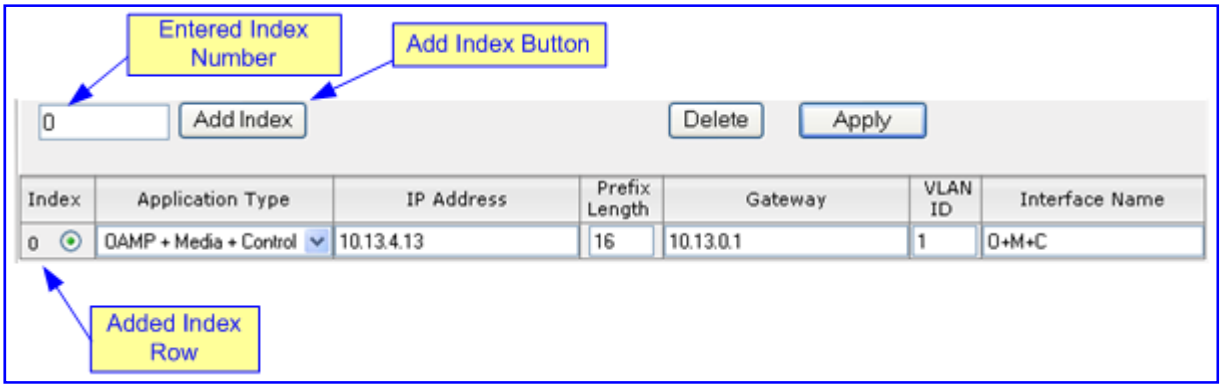
The Web interface includes many configuration pages that provide tables for configuring the device. Some of these tables provide the following command buttons:

- **Add Index:** adds an index entry to the table.
- **Duplicate:** duplicates a selected, existing index entry.
- **Compact:** organizes the index entries in ascending, consecutive order.
- **Delete:** deletes a selected index entry.
- **Apply:** saves the configuration.

➢ **To add an entry to a table:**

1. In the 'Add Index' field, enter the desired index entry number, and then click **Add Index**; an index entry row appears in the table:

Figure 3-11: Adding an Index Entry to a Table



2. Click **Apply** to save the index entry.

Notes:

- Before you can add another index entry, you must ensure that you have applied the previously added index entry (by clicking **Apply**).
- If you leave the 'Add' field blank and then click **Add Index**, the existing index entries are all incremented by one and the newly added index entry is assigned the index 0.

➢ **To add a copy of an existing index table entry:**

1. In the 'Index' column, select the index that you want to duplicate; the **Edit** button appears.
2. Click **Edit**; the fields in the corresponding index row become available.
3. Click **Duplicate**; a new index entry is added with identical settings as the selected index in Step 1. In addition, all existing index entries are incremented by one and the newly added index entry is assigned the index 0.

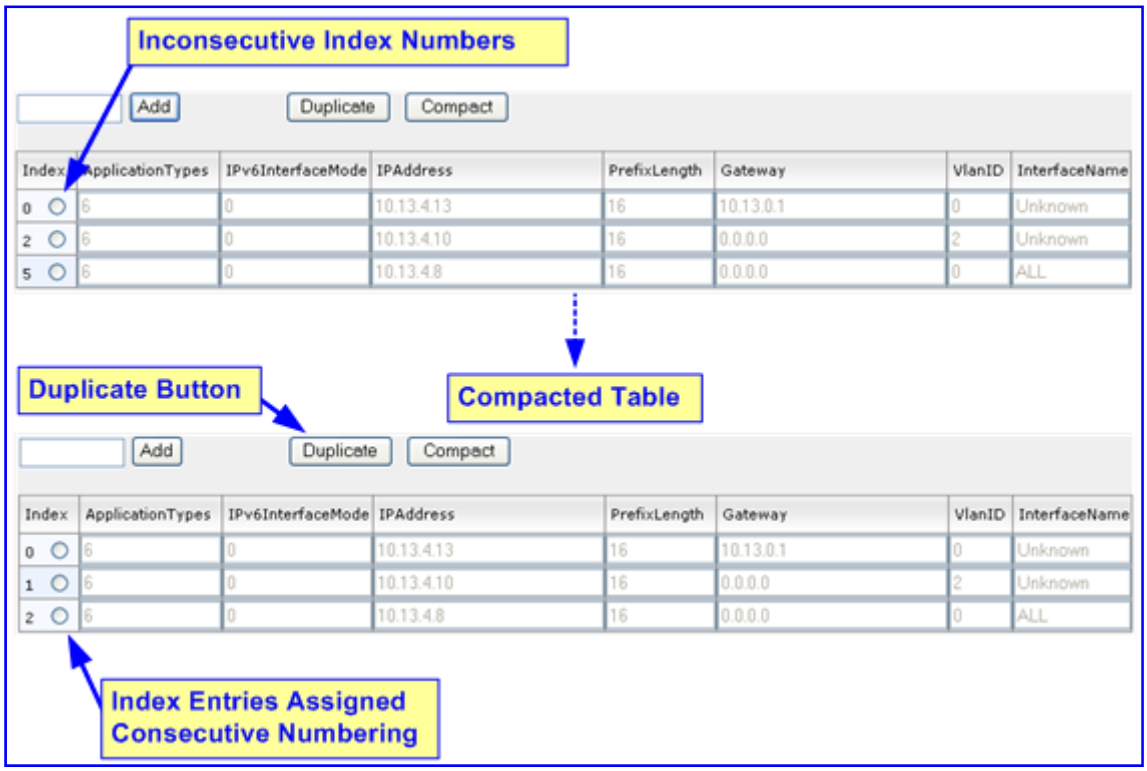
➢ **To edit an existing index table entry:**

1. In the 'Index' column, select the index corresponding to the table row that you want to edit.
2. Click **Edit**; the fields in the corresponding index row become available.
3. Modify the values as required, and then click **Apply**; the new settings are applied.

➢ **To organize the index entries in ascending, consecutive order:**

- Click **Compact**; the index entries are organized in ascending, consecutive order, starting from index 0. For example, if you added three index entries 0, 4, and 6, then the index entry 4 is re-assigned index number 1 and the index entry 6 is re-assigned index number 2.

Figure 3-12: Compacting a Web Interface Table



➢ **To delete an existing index table entry:**

1. In the 'Index' column, select the index corresponding to the table row that you want to delete.
2. Click **Delete**; the table row is removed from the table.

3.1.7 Searching for Configuration Parameters

The Web interface provides a search engine that allows you to search any *ini* file parameter that is configurable by the Web interface (i.e., has a corresponding Web parameter). You can search for a specific parameter (e.g., "EnableIPSec") or a sub-string of that parameter (e.g., "sec"). If you search for a sub-string, all parameters that contain the searched sub-string in their names are listed.

➢ **To search for *ini* file parameters configurable in the Web interface:**

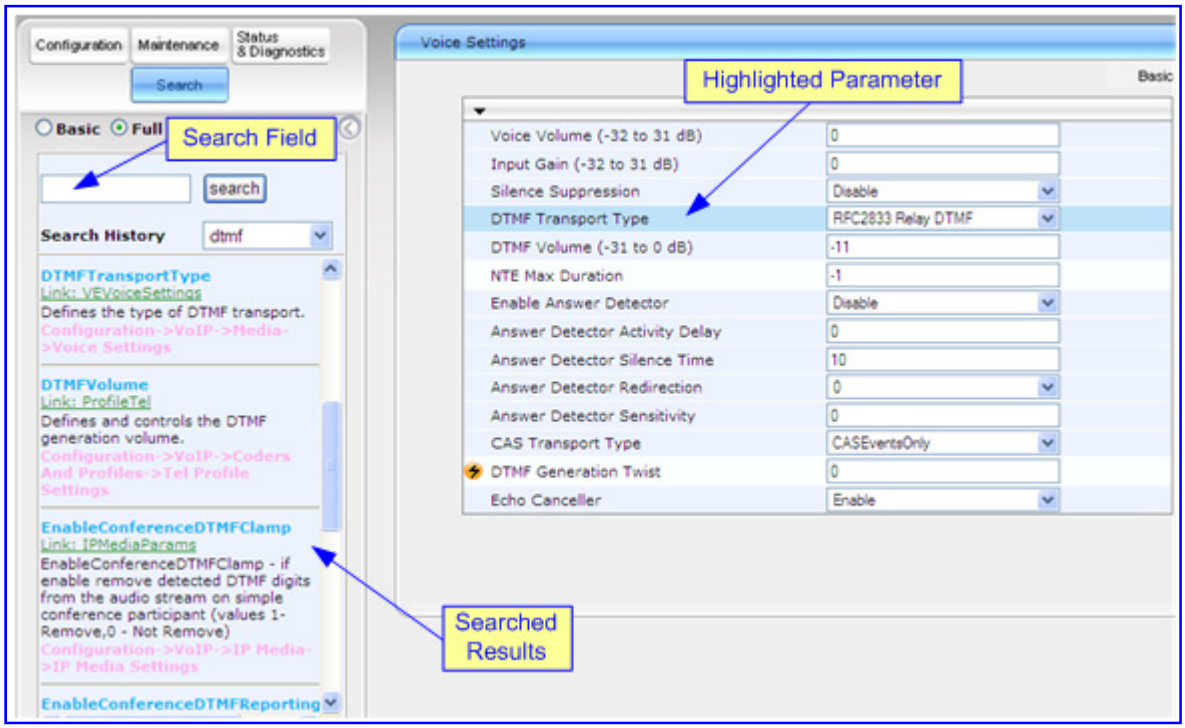
1. On the Navigation bar, click the **Search** tab; the Search engine appears in the Navigation pane.
2. In the 'Search' field, enter the parameter name or sub-string of the parameter name that you want to search. If you have performed a previous search for such a parameter, instead of entering the required 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 located parameters based on your search appears in the Navigation pane.

   Each searched result displays the following:

- *ini* file parameter name
- Link (in green) to its location (page) in the Web interface
- Brief description of the parameter

4. In the searched list, click the required parameter (link in green) to open the page in which the parameter appears; the relevant page opens in the Work pane and the searched parameter is highlighted for easy identification, as shown in the figure below:

Figure 3-13: Searched Result Screen



Note: If the searched parameter is not located, a notification message is displayed.

3.1.8 Working with Scenarios

The Web interface allows you to create your own "menu" with up to 20 pages selected from the menus in the Navigation tree (i.e., pertaining to the **Configuration**, **Maintenance**, and **Status & Diagnostics** tabs). The "menu" is a set of configuration pages grouped into a logical entity referred to as a *Scenario*. Each page in the Scenario is referred to as a *Step*. For each Step, you can select up to 25 parameters in the page that you want available in the Scenario. Therefore, the Scenario feature is useful in that it allows you quick-and-easy access to commonly used configuration parameters specific to your network environment. When you login to the Web interface, your Scenario is displayed in the Navigation tree, thereby, facilitating your configuration.

Instead of creating a Scenario, you can also load an existing Scenario from a PC to the device (see "Loading a Scenario to the Device" on page 48).

3.1.8.1 Creating a Scenario

The Web interface allows you to create one Scenario with up to 20 configuration pages, as described in the procedure below:

➢ **To create a Scenario:**

1. On the Navigation bar, click the **Scenarios** tab; a message box appears, requesting you to confirm creation of a Scenario:

Figure 3-14: Scenario Creation Confirm Message Box

Note: If a Scenario already exists, the Scenario Loading message box appears.

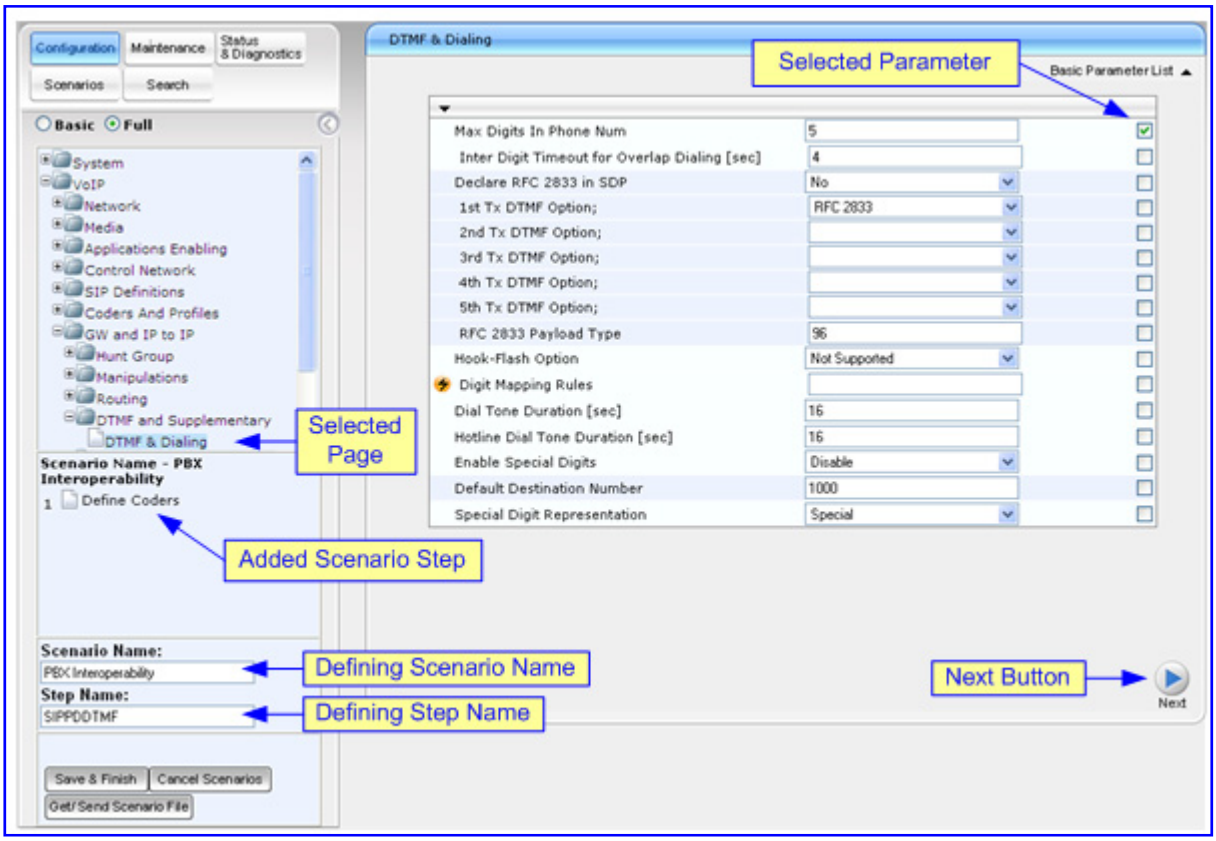
2. Click **OK**; the Scenario mode appears in the Navigation tree as well as the menus of the **Configuration** tab.

Note: If a Scenario already exists and you wish to create a new one, click the **Create Scenario** button, and then click **OK** in the subsequent message box.

3. In the 'Scenario Name' field, enter an arbitrary name for the Scenario.
4. On the Navigation bar, click the **Configuration** or **Maintenance** tab to display their respective menus in the Navigation tree.
5. In the Navigation tree, select the required page item for the Step, and then in the page itself, select the required parameters by selecting the check boxes corresponding to the parameters.
6. In the 'Step Name' field, enter a name for the Step.

7. Click the **Next** button located at the bottom of the page; the Step is added to the Scenario and appears in the Scenario Step list:

Figure 3-15: Creating a Scenario



8. Repeat steps 5 through 8 to add additional Steps (i.e., pages).
9. When you have added all the required Steps for your Scenario, click the **Save & Finish** button located at the bottom of the Navigation tree; a message box appears informing you that the Scenario has been successfully created.
10. Click **OK**; the Scenario mode is quit and the menu tree of the **Configuration** tab appears in the Navigation tree.

Notes:

- You can add up to 20 Steps to a Scenario, where each Step can contain up to 25 parameters.
- When in Scenario mode, the Navigation tree is in 'Full' display (i.e., all menus are displayed in the Navigation tree) and the configuration pages are in 'Advanced Parameter List' display (i.e., all parameters are shown in the pages). This ensures accessibility to all parameters when creating a Scenario. For a description on the Navigation tree views, see "Navigation Tree" on page 32.
- If you previously created a Scenario and you click the **Create Scenario** button, the previously created Scenario is deleted and replaced with the one you are creating.
- Only users with access level of 'Security Administrator' can create a Scenario.

3.1.8.2 Accessing a Scenario

Once you have created the Scenario, you can access it at anytime by following the procedure below:

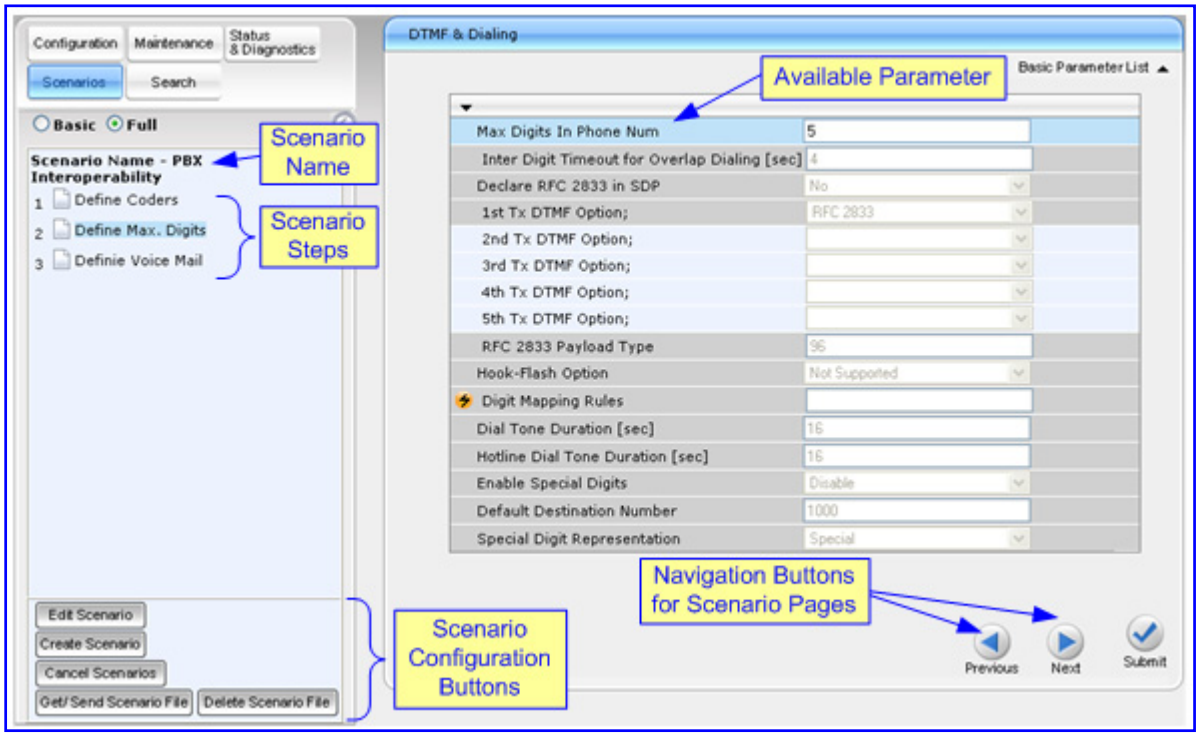
➢ **To access the Scenario:**

1. On the Navigation bar, select the **Scenario** tab; a message box appears, requesting you to confirm the loading of the Scenario.

Figure 3-16: Scenario Loading Message Box

2. Click **OK**; the Scenario and its Steps appear in the Navigation tree, as shown in the example figure below:

Figure 3-17: Scenario Example



When you select a Scenario Step, the corresponding page is displayed in the Work pane. In each page, the available parameters are indicated by a dark-blue background; the unavailable parameters are indicated by a gray or light-blue background.

To navigate between Scenario Steps, you can perform one of the following:

- In the Navigation tree, click the required Scenario Step.
- In an opened Scenario Step (i.e., page appears in the Work pane), use the following navigation buttons:
  - **Next:** opens the next Step listed in the Scenario.
  - **Previous**: opens the previous Step listed in the Scenario.

Note: If you reset the device while in Scenario mode, after the device resets, you are returned once again to the Scenario mode.

3.1.8.3 Editing a Scenario

You can modify a Scenario anytime by adding or removing Steps (i.e., pages) or parameters, and changing the Scenario name and the Steps' names.

Note: Only users with access level of 'Security Administrator' can edit a Scenario.

➢ **To edit a Scenario:**

1. On the Navigation bar, click the **Scenarios** tab; a message box appears, requesting you to confirm Scenario loading.
2. Click **OK**; the Scenario appears with its Steps in the Navigation tree.
3. Click the **Edit Scenario** button located at the bottom of the Navigation pane; the 'Scenario Name' and 'Step Name' fields appear.
4. You can perform the following edit operations:
   - **Add Steps:**
     a. On the Navigation bar, select the desired tab (i.e., **Configuration** or **Maintenance**); the tab's menu appears in the Navigation tree.
     b. In the Navigation tree, navigate to the desired page item; the corresponding page opens in the Work pane.
     c. In the page, select the required parameters, by marking their corresponding check boxes.
     d. Click **Next**.

- **Add or Remove Parameters:**
  a. In the Navigation tree, select the required Step; the corresponding page opens in the Work pane.
  b. To add parameters, select the check boxes corresponding to the desired parameters; to remove parameters, clear the check boxes corresponding to the parameters that you want removed.
  c. Click **Next**.
- **Edit the Step Name:**
  a. In the Navigation tree, select the required Step.
  b. In the 'Step Name' field, modify the Step name.
  c. In the page, click **Next**.
- **Edit the Scenario Name:**
  a. In the 'Scenario Name' field, edit the Scenario name.
  b. In the displayed page, click **Next**.
- **Remove a Step:**
  a. In the Navigation tree, select the required Step; the corresponding page opens in the Work pane.
  b. In the page, clear all the check boxes corresponding to the parameters.
  c. Click **Next**.

5. After clicking **Next**, a message box appears notifying you of the change. Click **OK**.
6. Click **Save & Finish**; a message box appears informing you that the Scenario has been successfully modified. The Scenario mode is exited and the menus of the **Configuration** tab appear in the Navigation tree.

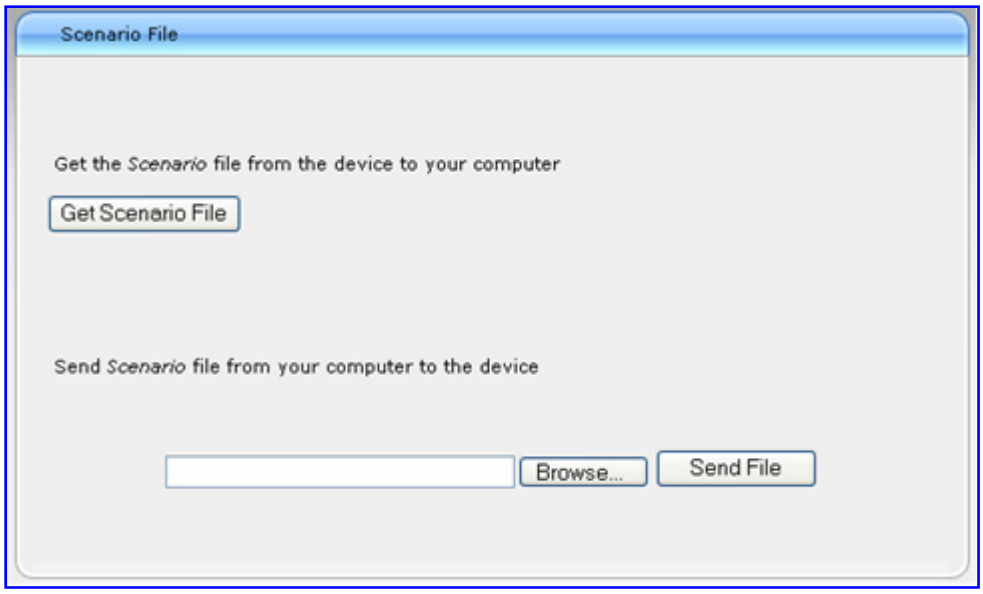
3.1.8.4 Saving a Scenario to a PC

You can save a Scenario to a PC (as a *dat* file). This is especially useful when requiring more than one Scenario to represent different environment setups (e.g., where one includes PBX interoperability and another not). Once you create a Scenario and save it to your PC, you can then keep on saving modifications to it under different Scenario file names. When you require a specific network environment setup, you can simply load the suitable Scenario file from your PC (see "Loading a Scenario to the Device" on page 48).

➢ **To save a Scenario to a PC:**

1. On the Navigation bar, click the **Scenarios** tab; the Scenario appears in the Navigation tree.
2. Click the **Get/Send Scenario File** button (located at the bottom of the Navigation tree); the 'Scenario File' page appears, as shown below:

Figure 3-18: Scenario File Page



3. Click the **Get Scenario File** button; the 'File Download' window appears.
4. Click **Save**, and then in the 'Save As' window navigate to the folder to where you want to save the Scenario file. When the file is successfully downloaded to your PC, the 'Download Complete' window appears.
5. Click **Close** to close the 'Download Complete' window.

3.1.8.5 Loading a Scenario to the Device

Instead of creating a Scenario, you can load a Scenario file (*data* file) from your PC to the device.

➢ **To load a Scenario to the device:**

1. On the Navigation bar, click the **Scenarios** tab; the Scenario appears in the Navigation tree.
2. Click the **Get/Send Scenario File** button (located at the bottom of the Navigation tree); the 'Scenario File' page appears (see "Saving a Scenario to a PC" on page 47).
3. Click the **Browse** button, and then navigate to the Scenario file stored on your PC.
4. Click the **Send File** button.

Notes:

- You can only load a Scenario file to a device that has an identical hardware configuration setup to the device in which it was created. For example, if the Scenario was created in a device with FXS interfaces, the Scenario cannot be loaded to a device that does not have FXS interfaces.
- The loaded Scenario replaces any existing Scenario.
- You can also load a Scenario file using BootP, by loading an ini file that contains the ini file parameter ScenarioFileName (see Web and Telnet Parameters on page 345). The Scenario dat file must be located in the same folder as the ini file. For a detailed description on BootP, refer to the Product Reference Manual.

3.1.8.6 Deleting a Scenario

You can delete the Scenario by using the **Delete Scenario File** button, as described in the procedure below:

➢ **To delete the Scenario:**

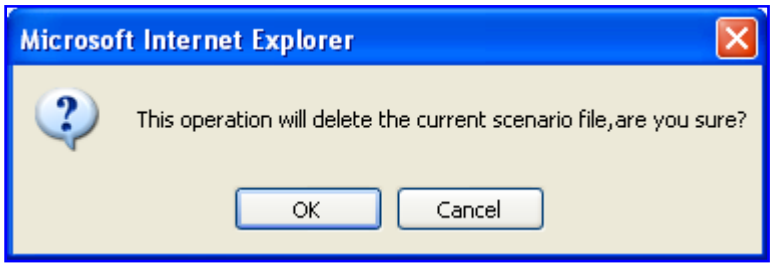
1. On the Navigation bar, click the **Scenarios** tab; a message box appears, requesting you to confirm:

Figure 3-19: Scenario Loading Message Box

2. Click **OK**; the Scenario mode appears in the Navigation tree.

3. Click the **Delete Scenario File** button; a message box appears requesting confirmation for deletion.

Figure 3-20: Message Box for Confirming Scenario Deletion



4. Click **OK**; the Scenario is deleted and the Scenario mode closes.

Note: You can also delete a Scenario using the following alternative methods:

- Loading an empty *dat* file (see "Loading a Scenario to the Device" on page 48).
- Loading an *ini* file with the ScenarioFileName parameter set to no value (i.e., ScenarioFileName = "").

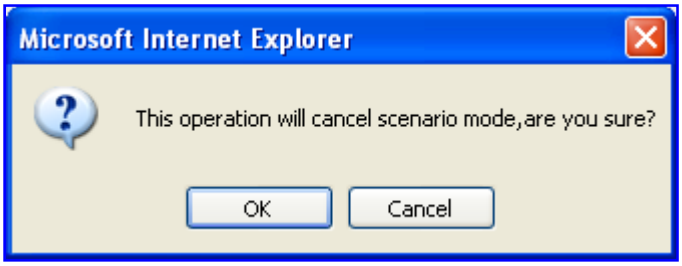
3.1.8.7 Exiting Scenario Mode

When you want to close the Scenario mode after using it for device configuration, follow the procedure below:

➢ **To close the Scenario mode:**

1. Simply click any tab (besides the **Scenarios** tab) on the Navigation bar, or click the **Cancel Scenarios** button located at the bottom of the Navigation tree; a message box appears, requesting you to confirm exiting Scenario mode, as shown below.

Figure 3-21: Confirmation Message Box for Exiting Scenario Mode



2. Click **OK** to exit.

3.1.9 Creating a Login Welcome Message

You can create a Welcome message box (alert message) that appears after each successful login to the device's Web interface. The *ini* file table parameter WelcomeMessage allows you to create the Welcome message. Up to 20 lines of character strings can be defined for the message. If this parameter is not configured, no Welcome message box is displayed after login.

An example of a Welcome message is shown in the figure below:

Figure 3-22: User-Defined Web Welcome Message after Login

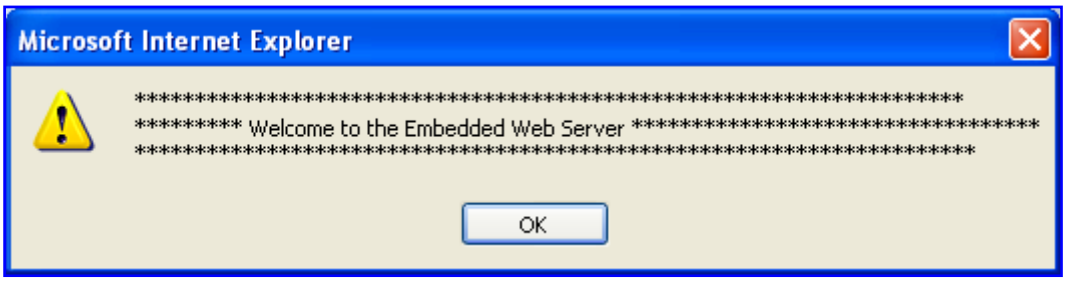


Table 3-2: ini File Parameter for Welcome Login Message

Parameter	Description
WelcomeMessage	Defines the Welcome message that appears after a successful login to the Web interface. The format of this parameter is as follows: [WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; [\WelcomeMessage] For Example: [WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; WelcomeMessage 1 = "**********"; WelcomeMessage 2 = "********* This is a Welcome message **"; WelcomeMessage 3 = "**********"; [\WelcomeMessage] **Note:** Each index represents a line of text in the Welcome message box. Up to 20 indices can be defined.

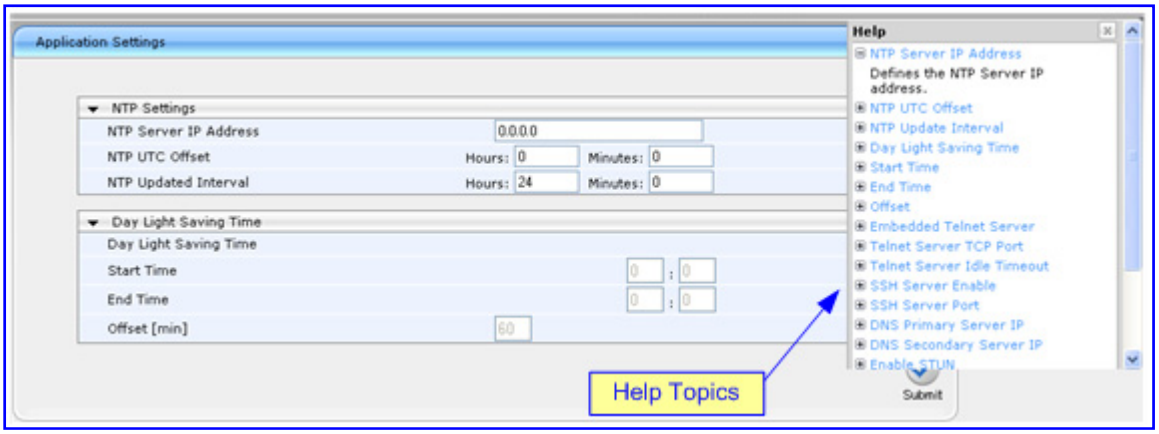
3.1.10 Getting Help

The Web interface provides you with context-sensitive Online Help. The Online Help provides you with brief descriptions of most of the parameters you'll need to successfully configure the device. The Online Help provides descriptions of parameters pertaining to the currently opened page.

➢ **To view the Help topic for a currently opened page:**

1. Using the Navigation tree, open the required page for which you want Help.
2. On the toolbar, click the **Help** button; the Help topic pertaining to the opened page appears, as shown below:

Figure 3-23: Help Topic for Current Page



3. To view a description of a parameter, click the **plus** ⊞ sign to expand the parameter. To collapse the description, click the **minus** ⊟ sign.
4. 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.

3.1.11 Logging Off the Web Interface

You can log off the Web interface and re-access it with a different user account. For detailed information on the Web User Accounts, see User Accounts.

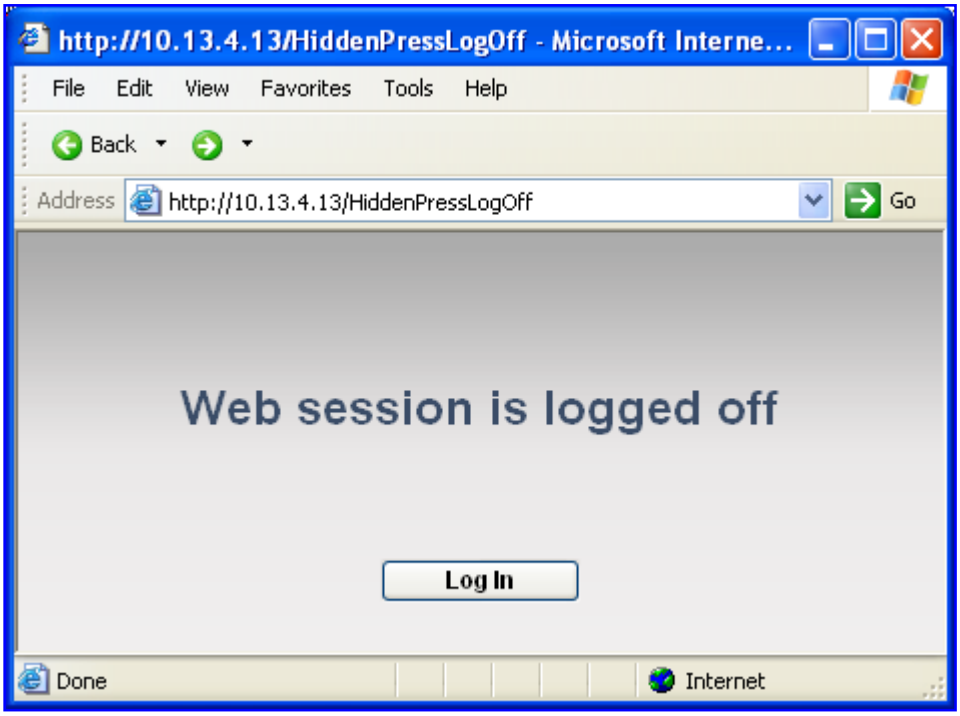
➢ **To log off the Web interface:**

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

Figure 3-24: Log Off Confirmation Box

2. Click **OK**; the Web session is logged off and the **Log In** button appears.

Figure 3-25: Web Session Logged Off



To log in again, simply click the **Log In** button, and then in the 'Enter Network Password' dialog box, enter your user name and password (see "Accessing the Web Interface" on page 28).

3.2 Using the Home Page

The 'Home' page provides you with a graphical display of the device's front panel, displaying color-coded status icons for monitoring the functioning of the device. The 'Home' page also displays general device information (in the 'General Information' pane) such as the device's IP address and firmware version.

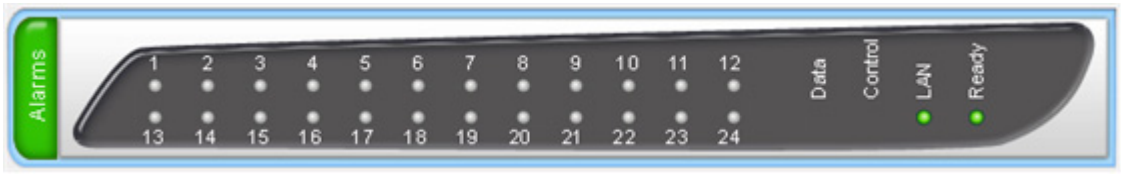
By default, the 'Home' page is displayed when you access the device's Web interface.

➢ **To access the Home page:**

- On the toolbar, click the **Home** icon; the 'Home' page is displayed.

Figure 3-26: MP-11x Home Page

Figure 3-27: MP-124 Home Page



Note: The displayed number and type (FXO and/or FXS) of channels depends on the device's model (e.g., MP-118 or MP-114).

In addition to the color-coded status information depicted on the graphical display of the device (as described in the subsequent table), 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
- **Analog Port Number:** number of analog (FXS and FXO) ports
- **Firmware Version:** software version currently running on the device
- **Protocol Type:** signaling protocol currently used by the device (i.e. SIP)
- **Gateway Operational State:** operational state of the device:
  - 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 "Maintenance Actions" on page 166.

The table below describes the areas of the 'Home' page.

Table 3-3: Description of the Areas of the Home Page

Label	Description
Alarms	Displays the highest severity of an active alarm raised (if any) by the device: ▪ Green = no alarms ▪ Red = Critical alarm ▪ Orange = Major alarm ▪ Yellow = Minor alarm To view a list of active alarms in the 'Active Alarms' page (see "Viewing Active Alarms" on page 183), click the Alarms area.
Channel/Ports	Displays the status of the ports (channels): ▪ (red): line not connected (only applicable to FXO devices) ▪ (grey): channel inactive ▪ (blue): handset is off-hook ▪ (green): active RTP stream You can also view the channel's port settings (see "Viewing Analog Port Information" on page 56), reset the port (see "Resetting an Analog Channel" on page 55), and assign a name to the port (see "Assigning a Port Name" on page 55).
Uplink (MP-11x) **LAN (MP-124**	If clicked, the 'Ethernet Port Information' page opens, displaying Ethernet port configuration settings (see "Viewing Ethernet Port Information" on page 182).
Fail	Currently not supported.
Ready	Currently not supported.
Power	Always lit green, indicating power received by the device.

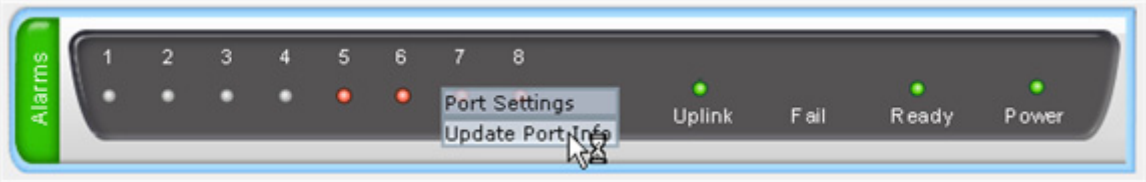
3.2.1 Assigning a Port Name

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.

➢ **To add a port description:**

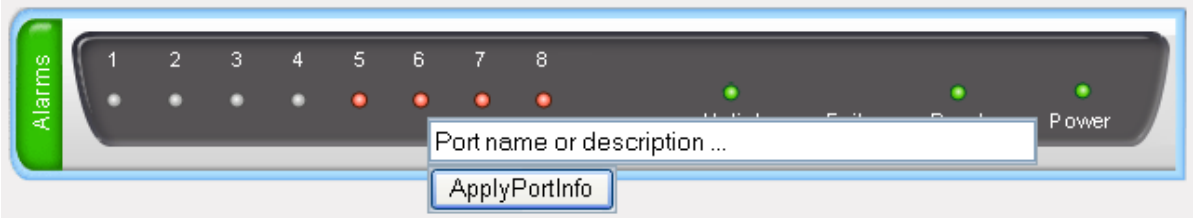
1. Click the required port icon; a shortcut menu appears, as shown below:

Figure 3-28: Shortcut Menu (e.g. MP-11x)



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

Figure 3-29: Typing Port Name (e.g. MP-11x)



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

3.2.2 Resetting an Analog Channel

The 'Home' page allows you to 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).

➢ **To reset a channel:**

- Click the required **FXS** or **FXO** port icon, and then from the shortcut menu, choose **Reset Channel**; the channel is changed to inactive (i.e., the port icon is displayed in grey).

Figure 3-30: Shortcut Menu (e.g. MP-11x)

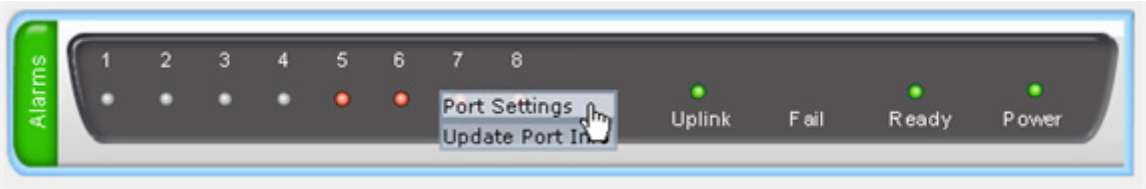
3.2.3 Viewing Analog Port Information

The 'Home' page allows you to view detailed information on a specific FXS or FXO analog port such as RTP/RTCP and voice settings.

➢ **To view detailed port information:**

1. Click the port for which you want to view port settings; the shortcut menu appears.

Figure 3-31: Shortcut Menu (e.g. MP-11x)



2. From the shortcut menu, click **Port Settings**; the 'Basic Channel Information' page appears.

Figure 3-32: Basic Channel Information Page

SIP ◆ Basic ◆ RTP/RTCP ◆ Voice Settings

Channel Identifier:	4
Status:	Inactive
Call ID:	0
Endpoint ID:	
Call Duration [sec]:	0
Call Type:	Voice
Call Destination:	10.13.4.13
Coder:	G711Alaw_64
Last Current Disconnect Duration:	0
Line Current[mA]:	0
Line Voltage[V]:	0
Hook(0-Onhook, 1-Off hook):	0
Ring(0-Off, 1-On):	0
Line Connected(0-Disconnected, 1-Connected):	0
Polarity state(0-Normal, 1-Reversed, 2-N\A):	0
Line polarity(0-Positive, 1-Negative):	0
Message Waiting Indication(0-Off, 1-On):	0

3. To view RTP/RTCP or voice settings, click the relevant button.

3.3 Configuration Tab

The **Configuration** tab on the Navigation bar displays menus in the Navigation tree related to device configuration. This tab provides the following main menus:

- System (see "System Settings" on page 57)
- VoIP (see "VoIP Settings" on page 78)

3.3.1 System Settings

The **System** menu includes the following:

- Application Settings item (see "Configuring Application Settings" on page 58)
- Syslog Settings item (see "Configuring Syslog Settings" on page 61)
- Regional Settings item (see "Configuring Regional Settings" on page 62)
- Certificates item (see "Configuring Certificates" on page 62)
- Management submenu (see "Management Settings" on page 66)

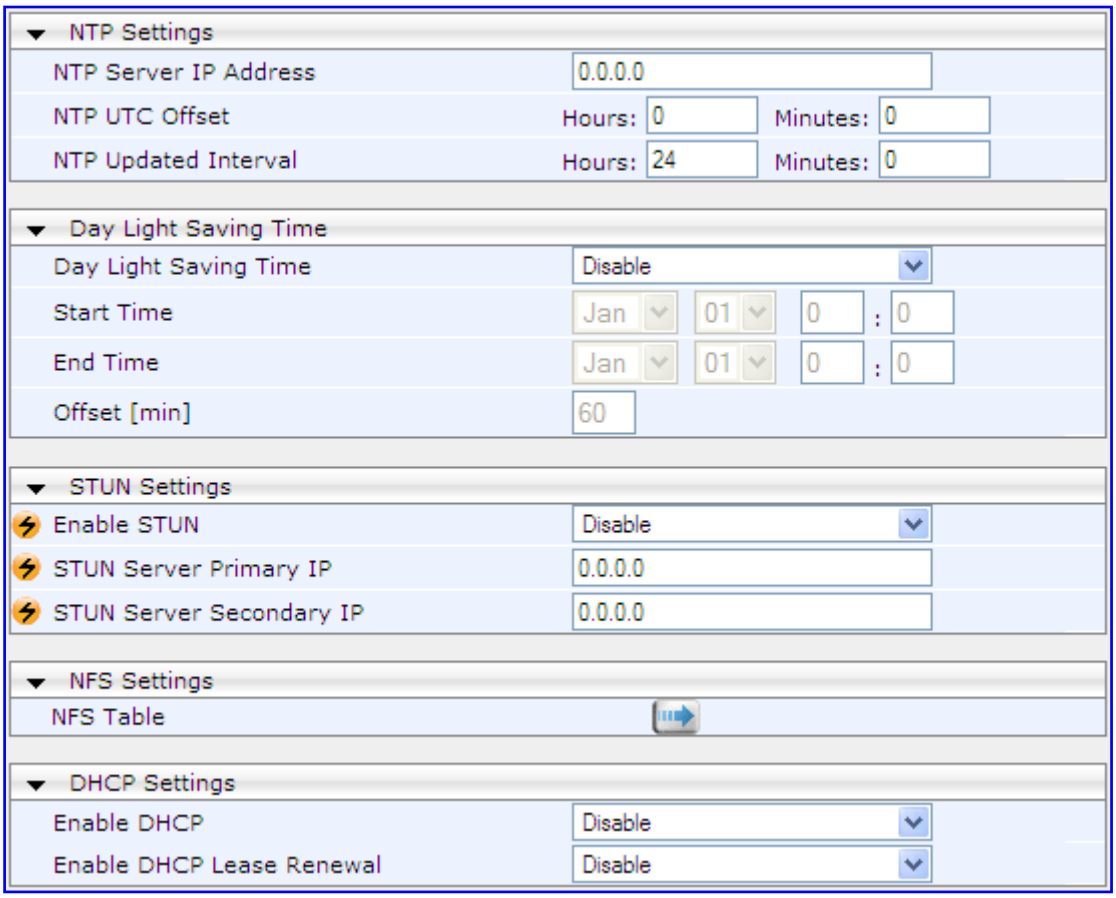
3.3.1.1 Configuring Application Settings

The 'Application Settings' page is used for configuring various application parameters such as Network Time Protocol (NTP), daylight saving time, and Network File System (NFS). For a description of these parameters, see "Configuration Parameters Reference" on page 333.

➢ **To configure application settings:**

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

Figure 3-33: Application Settings Page



2. Configure the parameters as required.
3. For configuring NFS, under the 'NFS Settings' group, click the **NFS Table** button; the 'NFS Settings' page appears. For a description of configuring this page, see "Configuring NFS Settings" on page 59.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.

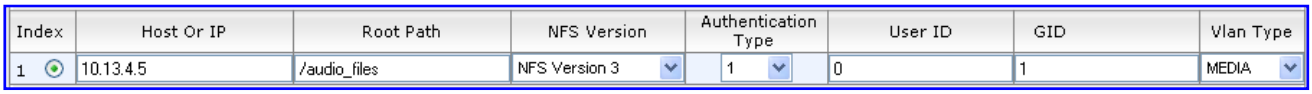
3.3.1.2 Configuring NFS Settings

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. 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. NFS is used by the device to load the *cmp*, *ini*, and auxiliary files, using the Automatic Update mechanism (refer to the *Product Reference Manual*). 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 (see "Configuring Application Settings" on page 58).
2. Under the NFS Settings group, click the **NFS Table** button; the 'NFS Settings' page appears.

Figure 3-34: NFS Settings Page



3. In the 'Add' field, enter the index number of the remote NFS file system, and then click **Add**; an empty entry row appears in the table.
4. Configure the NFS parameters according to the table below.
5. Click the **Apply** 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 169.

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.
- For an explanation on configuring Web interface tables, see "Working with Tables" on page 39.
- You can also configure the NFS table using the *ini* file table parameter NFSServers (see "NFS Parameters" on page 341).

Table 3-4: NFS Settings Parameters

Parameter	Description
Index	The row index of the remote file system. The valid range is 1 to 16.
Host Or IP	The domain name or IP address of the NFS server. If a domain name is provided, a DNS server must be configured.
Root Path	Path to the root of the remote file system in the format: /[path]. For example, '/audio'.
NFS Version	NFS version used to access the remote file system. ▪ **[2]** NFS Version 2 ▪ **[3]** NFS Version 3 (default)
Authentication Type	Authentication method used for accessing the remote file system. ▪ **[0]** Null ▪ **[1]** Unix (default)
User ID	User ID used in authentication when using Unix. The valid range is 0 to 65537. The default is 0.
Group ID	Group ID used in authentication when using Unix. The valid range is 0 to 65537. The default is 1.
VLAN Type	The VLAN type for accessing the remote file system. ▪ **[0]** OAM ▪ **[1]** MEDIA (default) **Note:** This parameter applies only if VLANs are enabled or if Multiple IPs is configured (see "Network Configuration" on page 316).

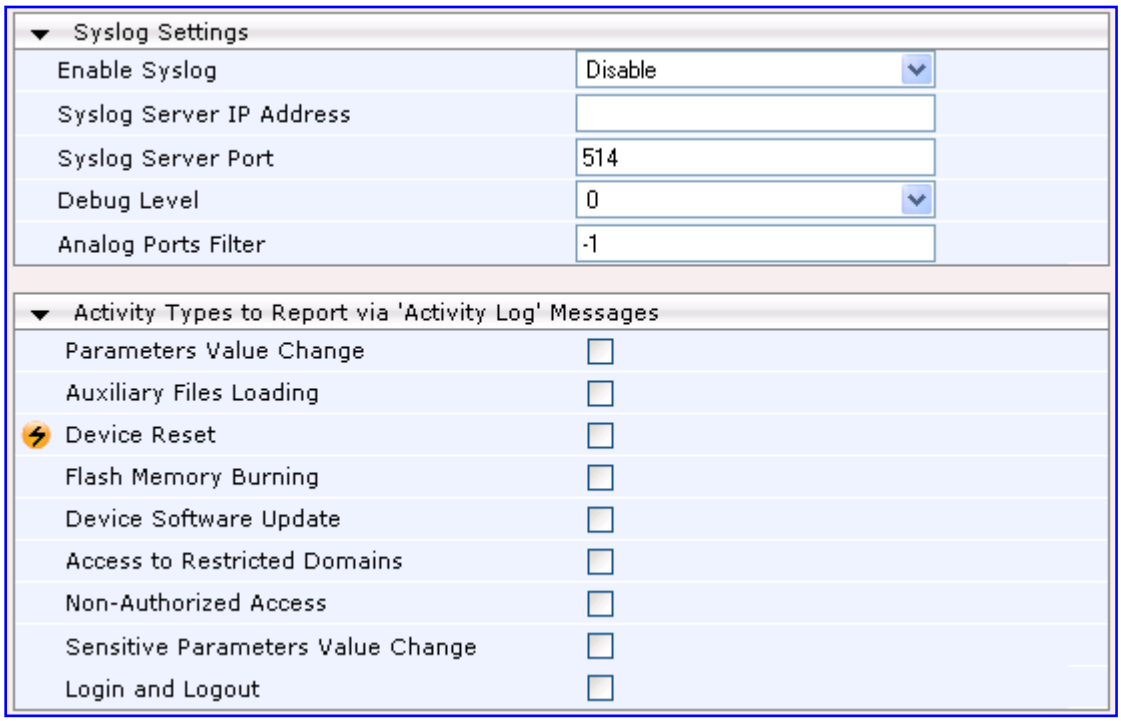
3.3.1.3 Configuring Syslog Settings

The 'Syslog Settings' page allows you to configure the device's embedded Syslog client. For a detailed description on the Syslog parameters, see "Syslog, CDR and Debug Parameters" on page 350. For viewing Syslog messages in the Web interface, see Viewing Syslog Messages on page 180. For a detailed description on Syslog messages and using third-party Syslog servers, refer to the *Product Reference Manual*.

➢ **To configure the Syslog client:**

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

Figure 3-35: Syslog Settings Page



2. Configure the parameters as required, and then click the **Submit** button to apply your changes.
3. To save the changes to flash memory, see "Saving Configuration" on page 169.

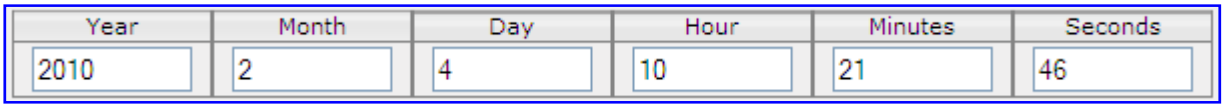
3.3.1.4 Configuring Regional Settings

The 'Regional Settings' page allows you to define and view the device's internal date and time.

➢ **To configure the device's date and time:**

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

Figure 3-36: Regional Settings Page



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

Notes:

- If the device is configured to obtain the date and time from an SNTP server (see "Configuring Application Settings" on page 58), the fields on this page are read-only and cannot be modified.
- For an explanation on SNTP, see "Simple Network Time Protocol Support" on page 315.
- After performing a hardware reset, the date and time are returned to their defaults and therefore, should be updated.

3.3.1.5 Configuring Certificates

The 'Certificates' page is used for HTTPS and SIP TLS secure communication. This page allows you to perform the following:

- Replacing the server certificate (see "Server Certificate Replacement" on page 62)
- Replacing the client certificates (see "Client Certificates" on page 65)
- Regenerating Self-Signed Certificates (see "Self-Signed Certificates" on page 66)
- Automatic update of the Private key (installed automatically from a file located on an HTTPS server, defined using the HTTPSPkeyFileName parameter). For a detailed description on automatic update methods, refer to the *Product Reference Manual*.

Note: The device is shipped with a configured certificate, therefore, configure certificates only if required.

3.3.1.5.1 Server Certificate Replacement

The device is supplied with a working Secure Socket Layer (SSL) 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 self-signed 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 HTTPSOnly parameter to 'HTTP and HTTPS' (0) - see "Configuring Web Security Settings" on page 69. This ensures that you have a method for accessing the device in case the new certificate doesn't work. Restore the previous setting after testing the configuration.
3. Open the 'Certificates Signing Request' page (**Configuration** tab > **System** menu > **Certificates**).

Figure 3-37: Certificates Signing Request Page

4. In the 'Subject Name' field, enter the DNS name, and then click **Generate CSR**. A textual certificate signing request that contains the SSL device identifier is displayed.
5. Copy this 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/MQswCQYDVQQGEwJGUj
ETMBEGA1UEChMKQ2VydGlwb3N0ZTEbMBkGA1UEAxMSQ2VydGlwb3N0ZSBTZXJ2ZXVy
MB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRlIxEz
ARBgNVBAoTCkNlcnRpcG9zdGUxGzAZBgNVBAMTEkNlcnRpcG9zdGUgU2VydmV1cjCC
ASEwDQYJKoZIhvcNAQEBBQADggEOADCCAQkCggEAPqd4MziR4spWldGRx8bQrhZkon
WnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7
JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRefiXDmuOe+FhJ
gHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUP1F1jMa+LPwvREXfFcUW+w==
-----END CERTIFICATE-----
```

7. In the 'Certificates Files' group, click the **Browse** button corresponding to 'Send Server Certificate...', navigate to the cert.txt file, and then click **Send File**.

8. When the certificate has successfully loaded, save the configuration (see "Saving Configuration" on page 169) and restart the device; the Web interface uses the provided certificate.
9. If the device was originally operating in HTTPS mode and you disabled it in Step 2, then return it to HTTPS by setting the parameter 'Secured Web Connection (HTTPS)' to 'HTTPS Only' (1) - see "Configuring Web Security Settings" on page 69.

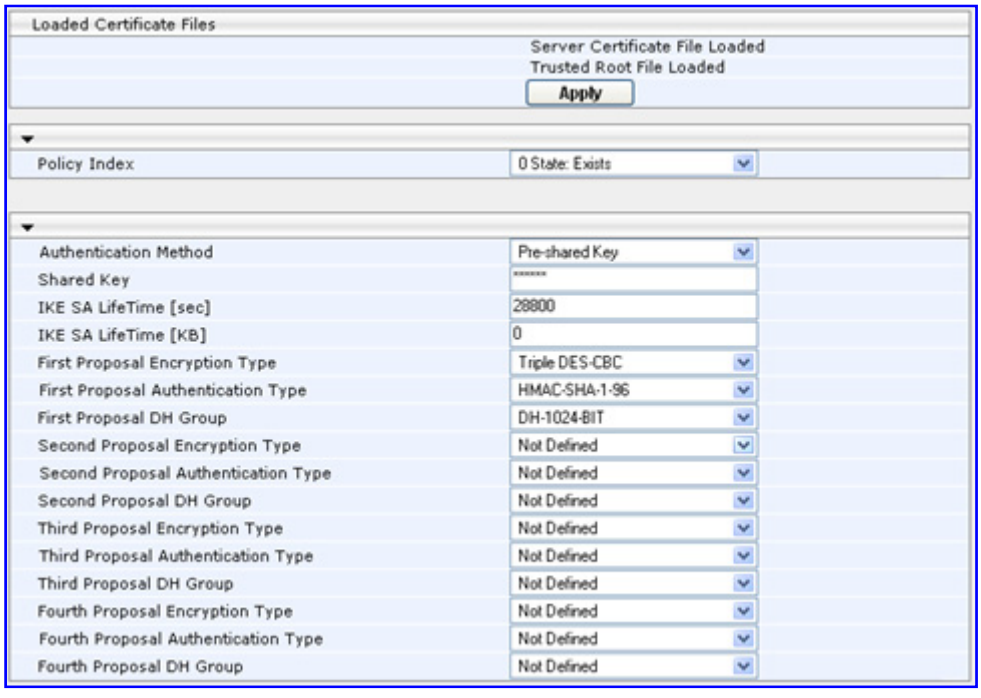
Notes:

- 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 changes and may not uniquely identify the device.
- The server certificate can also be loaded via *ini* file using the parameter HTTPSCertFileName.

➢ **To apply the loaded certificate for IPSec negotiations:**

1. Open the 'IKE Table' page (see Configuring the IP Security Proposal Table on page 94); the 'Loaded Certificates Files' group lists the newly uploaded certificates, as shown below:

Figure 3-38: IKE Table Listing Loaded Certificate Files



2. Click the Apply button to load the certificates; future IKE negotiations are now performed using the new certificates.

3.3.1.5.2 Client Certificates

By default, Web servers using SSL provide one-way authentication. The client is certain that the information provided by the Web 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 same certificate (in base64-encoded X.509 format) to the device's Trusted Root Certificate Store. The Trusted Root Certificate file should contain both the certificate of the authorized user and the certificate of the CA.

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 315) to obtain the current date and time. Without the correct date and time, client certificates cannot work.

➢ **To enable two-way client certificates:**

1. Set the parameter 'Secured Web Connection (HTTPS)' to 'HTTPS Only' (0) in "Configuring Web Security Settings" on page 69 to ensure you have a method of accessing the device in case the client certificate doesn't work. Restore the previous setting after testing the configuration.
2. Open the 'Certificates Signing Request' page (see "Server Certificate Replacement" on page 62).
3. In the 'Certificates Files' group, click the **Browse** button corresponding to 'Send "Trusted Root Certificate Store" file ...', navigate to the file, and then click **Send File**.
4. When the operation is complete, set the HTTPSRequireClientCertificate *ini* file parameter to 1.
5. Save the configuration (see "Saving Configuration" on page 169), and then restart the device.

When a user connects to the secured Web server:

- 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 doesn't have a client certificate from a listed CA, or doesn't have a client certificate at all, 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 Web browser or operating system documentation, and/or consult your security administrator.
- The root certificate can also be loaded via *ini* file using the parameter HTTPSRootFileName.
- You can enable Online Certificate Status Protocol (OCSP) on the device to check whether a peer's certificate has been revoked by an OCSP server. For further information, refer to the *Product Reference Manual*.

3.3.1.5.3 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 "Server Certificate Replacement" on page 62).
3. In the 'Subject Name' field, enter the fully-qualified DNS name (FQDN) as the certificate subject, and then click **Generate Self-signed**; after a few seconds, a message appears displaying the new subject name.
4. Save configuration (see "Saving Configuration" on page 169), and then restart the device for the new certificate to take effect.

3.3.1.6 Management Settings

The **Management** submenu includes the following:

- WEB User Accounts item (see "Configuring Web User Accounts" on page 66)
- Web Security Settings item (see "Configuring Web Security Settings" on page 69)
- Telnet/SSH Settings item (see "Configuring Telnet and SSH Settings" on page 70)
- WEB & Telnet Access List item (see "Configuring Web and Telnet Access List" on page 70)
- RADIUS Settings item (see "Configuring RADIUS Settings" on page 72)
- SNMP settings submenu (see "SNMP Settings" on page 73)

3.3.1.6.1 Configuring Web User Accounts

To prevent unauthorized access to the Web interface, two Web user accounts are available (primary and secondary) with assigned user name, password, and access level. When you login to the Web interface, you are requested to provide the user name and password of one of these Web user accounts. 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 user name and password. Up to five Web users can simultaneously open (log in to) a session on the device's Web interface.

Each Web user account is composed of three attributes:

- **User name and password:** enables access (login) to the Web interface.
- **Access level:** determines the extent of the access (i.e., availability of pages and read / write privileges). The available access levels and their corresponding privileges are listed in the table below:

Table 3-5: Web User Accounts Access Levels and Privileges

Access Level	Numeric Representation*	Privileges
Security Administrator	200	Read / write privileges for all pages.
Administrator	100	read / write privileges for all pages except security-related pages, which are read-only.
User Monitor	50	No access to security-related and file-loading pages; read-only access to the other pages. This read-only access level is typically applied to the secondary Web user account.
No Access	0	No access to any page.
* 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).		

The default attributes for the two Web user accounts are shown in the following table:

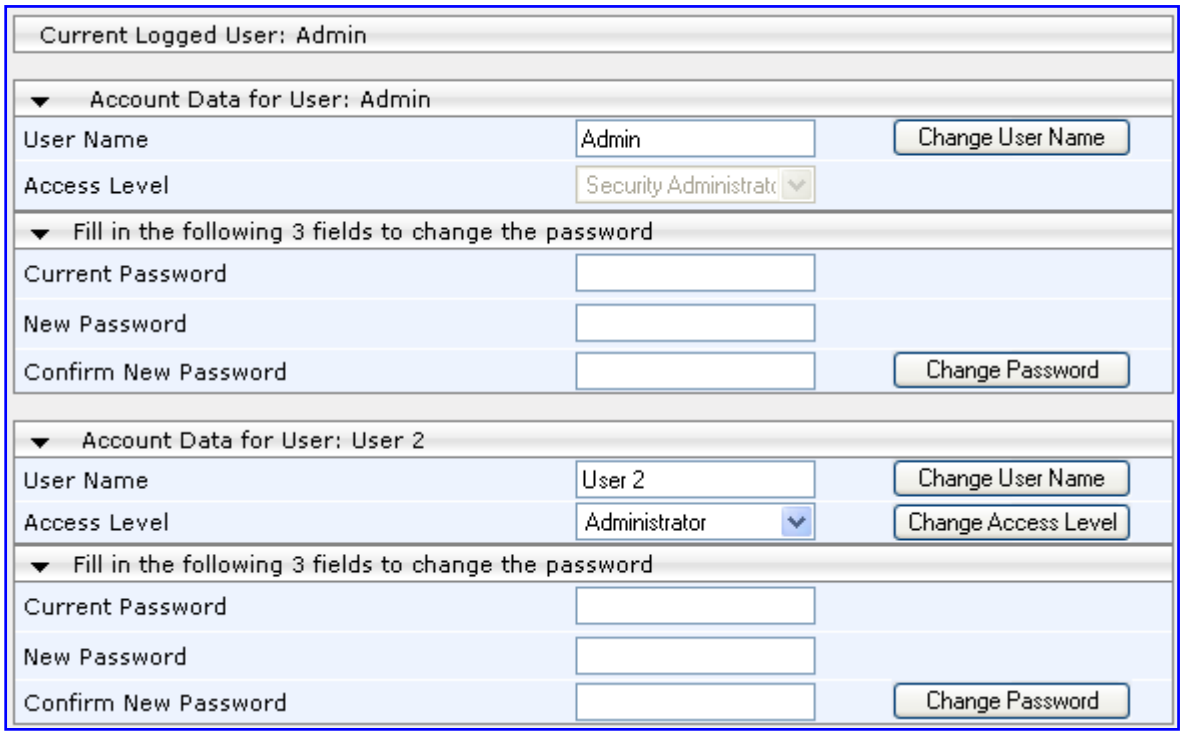
Table 3-6: Default Attributes for the Web User Accounts

Account / Attribute	User Name (Case-Sensitive)	Password (Case-Sensitive)	Access Level
Primary Account	Admin	Admin	Security Administrator **Note:** The Access Level cannot be changed for this account type.
Secondary Account	User	User	User Monitor

➢ **To change the Web user accounts attributes:**

1. Open the 'Web User Accounts' page (**Configuration** tab > **System** menu > **Web User Accounts**).

Figure 3-39: WEB User Accounts Page (for Users with 'Security Administrator' Privileges)



Note: If you are logged into the Web interface as the Security Administrator, both Web user accounts are displayed on the 'Web User Accounts' page (as shown above). If you are logged in with the secondary user account, only the details of the secondary account are displayed on the page.

2. To change the access level of the secondary account:
   a. From the 'Access Level' drop-down list, select the new access level.
   b. Click **Change Access Level**; the new access level is applied immediately.

Notes:

- The access level of the primary Web user account is 'Security Administrator', which cannot be modified.
- The access level of the secondary account can only be modified by the primary account user or a secondary account user with 'Security Administrator' access level.

3. To change the user name of an account, perform the following:
   a. In the field 'User Name', enter the new user name (maximum of 19 case-sensitive characters).
   b. Click **Change User Name**; if you are currently logged into the Web interface with this account, the 'Enter Network Password' dialog box appears, requesting you to enter the new user name.
4. To change the password of an account, perform the following:
   a. In the field 'Current Password', enter the current password.
   b. In the fields 'New Password' and 'Confirm New Password', enter the new password (maximum of 19 case-sensitive characters).

c. Click **Change Password**; if you are currently logged into the Web interface with this account, the 'Enter Network Password' dialog box appears, requesting you to enter the new password.

Notes:

- For security, it's recommended that you change the default user name and password.
- A Web user with access level 'Security Administrator' can change all attributes of all the Web user accounts. Web users with an access level other than 'Security Administrator' can only change their own password and user name.
- To reset the two Web user accounts' user names and passwords to default, set the *ini* file parameter ResetWebPassword to 1.
- To access the Web interface with a different account, click the **Log off** button located on the toolbar, click any button or page item, and then re-access the Web interface with a different user name and password.
- You can set the entire Web interface to read-only (regardless of Web user account's access level), by using the *ini* file parameter DisableWebConfig (see "Web and Telnet Parameters" on page 345).
- Access to the Web interface can be disabled, by setting the ini file parameter DisableWebTask to 1. By default, access is enabled.
- You can define additional Web user accounts using a RADIUS server (refer to the *Product Reference Manual*).
- For secured HTTP connection (HTTPS), refer to the *Product Reference Manual*.

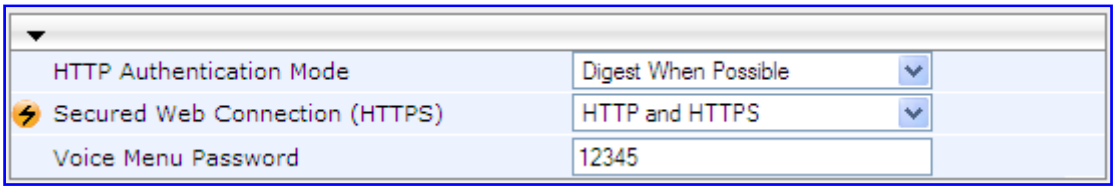
3.3.1.6.2 Configuring Web Security Settings

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 345.

➢ **To define Web access security:**

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

Figure 3-40: WEB Security Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

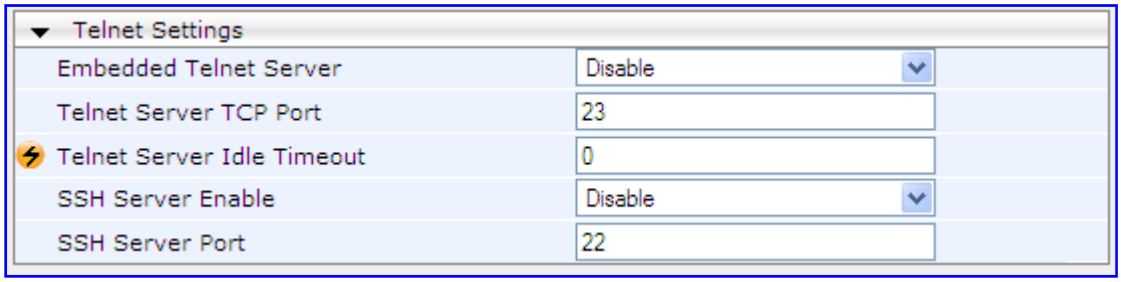
3.3.1.6.3 Configuring Telnet and SSH Settings

The 'Telnet/SSH Settings' page is used to define Telnet and Secure Shell (SSH). For a description of these parameters, see "Web and Telnet Parameters" on page 345.

➢ **To define Telnet and SSH:**

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

Figure 3-41: Telnet/SSH Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

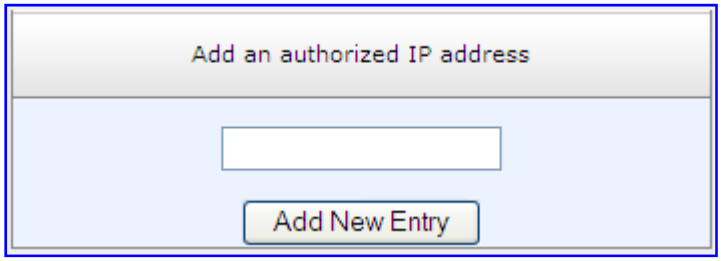
3.3.1.6.4 Configuring Web and Telnet Access List

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 345).

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

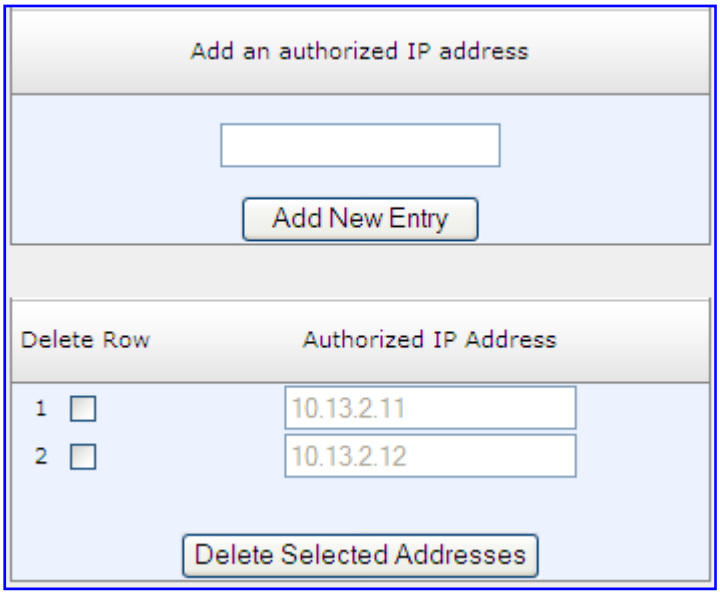
1. Open the 'Web & Telnet Access List' page (**Configuration** tab > **System** menu > **Management** submenu > **Web & Telnet Access List**).

Figure 3-42: 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 3-43: Web & Telnet Access List Table



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 169.

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.

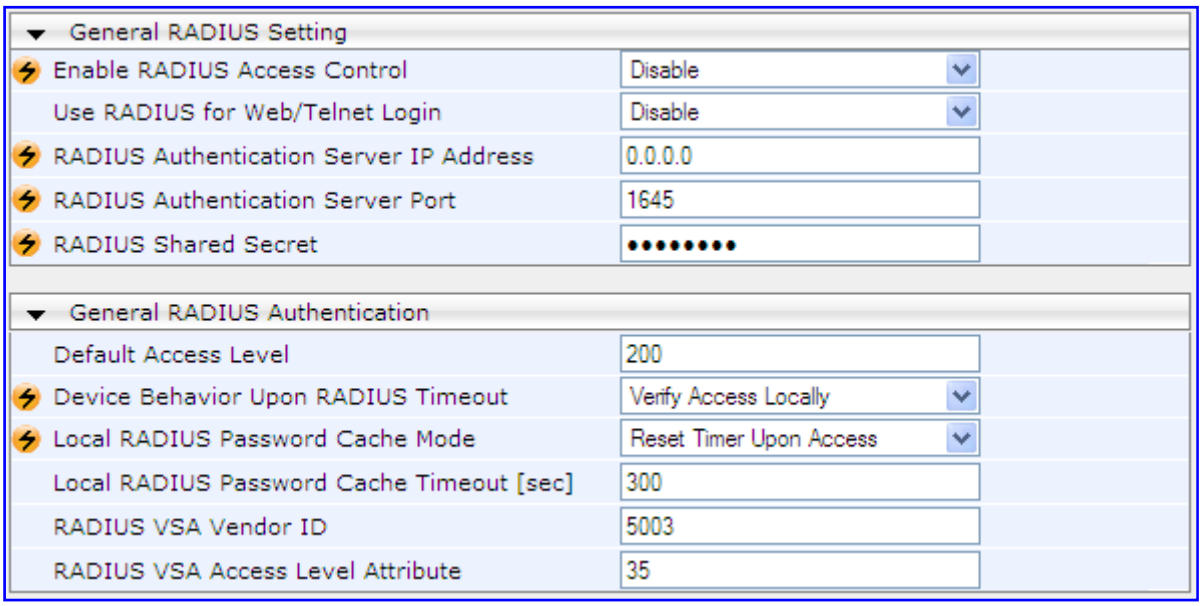
3.3.1.6.5 Configuring RADIUS Settings

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 333.

➢ **To configure RADIUS:**

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

Figure 3-44: RADIUS Parameters Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.1.6.6 SNMP Settings

The **SNMP** submenu includes the following items:

- SNMP Community Settings (see "Configuring SNMP Community Strings" on page 73)
- SNMP Trap Destinations (see "Configuring SNMP Trap Destinations" on page 74)
- SNMP Trusted Managers (see "Configuring SNMP Trusted Managers" on page 75)
- SNMP V3 Users (see "Configuring SNMP V3 Users" on page 76)

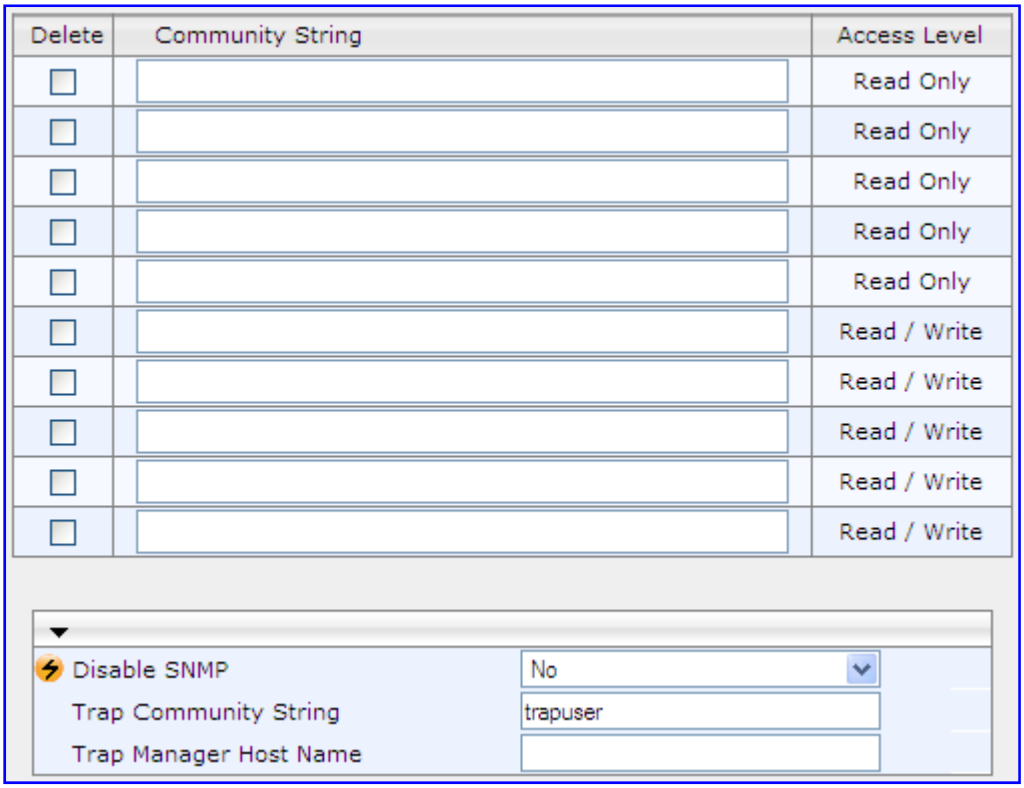
3.3.1.6.6.1 Configuring SNMP Community Strings

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 information on SNMP community strings, refer to the *Product Reference Manual*. For detailed description on the SNMP parameters, see "SNMP Parameters" on page 366.

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

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

Figure 3-45: SNMP Community String Page



2. Configure the SNMP community strings parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

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

Table 3-7: SNMP Community String Parameters Description

Parameter	Description
Community String	▪ Read Only [SNMPReadOnlyCommunityString_x]: Up to five read-only community strings (up to 19 characters each). The default string is 'public'. ▪ Read / Write [SNMPReadWriteCommunityString_x]: Up to five read / write community strings (up to 19 characters each). The default string is 'private'.
Trap Community String **[SNMPTrapCommunityString]**	Community string used in traps (up to 19 characters). The default string is 'trapuser'.

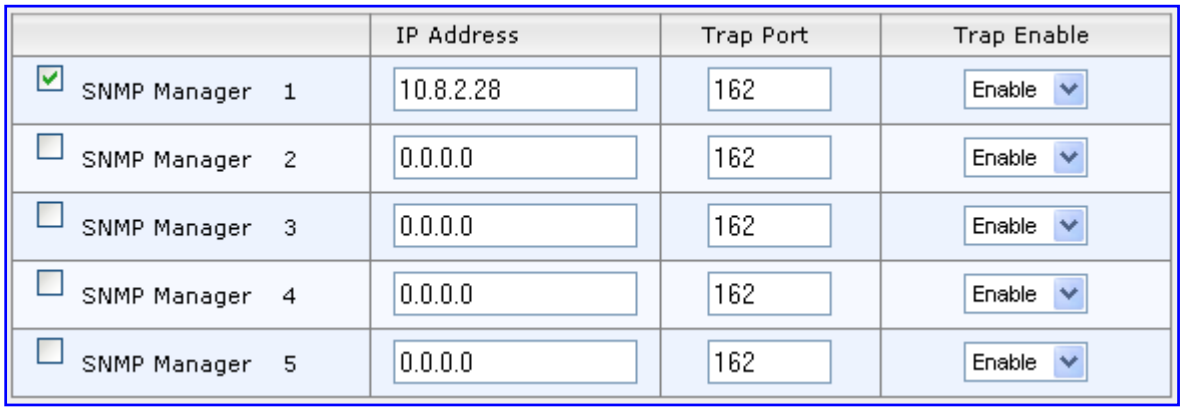
3.3.1.6.6.2 Configuring SNMP Trap Destinations

The 'SNMP Trap Destinations' page allows you to configure up to five SNMP trap managers.

➢ **To configure SNMP trap destinations:**

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

Figure 3-46: SNMP Trap Destinations Page



2. Configure the SNMP trap managers parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

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

Table 3-8: SNMP Trap Destinations Parameters Description

Parameter	Description
SNMP Manager **[SNMPManagerIsUsed_x]**	Determines the validity of the parameters (IP address and port number) of the corresponding SNMP Manager used to receive SNMP traps. ▪ **[0]** (Check box cleared) = Disabled (default) ▪ **[1]** (Check box selected) = Enabled

Parameter	Description
IP Address **[SNMPManagerTableIP_x]**	IP address of the remote host used as an SNMP Manager. The device sends SNMP traps to these IP addresses. Enter the IP address in dotted-decimal notation, e.g., 108.10.1.255.
Trap Port **[SNMPManagerTrapPort_x]**	Defines the port number of the remote SNMP Manager. The device sends SNMP traps to these ports. The valid SNMP trap port range is 100 to 4000. The default port is 162.
Trap Enable **[SNMPManagerTrapSendingEnable_x]**	Activates or de-activates the sending of traps to the corresponding SNMP Manager. ▪ **[0]** Disable = Sending is disabled. ▪ **[1]** Enable = Sending is enabled (default).

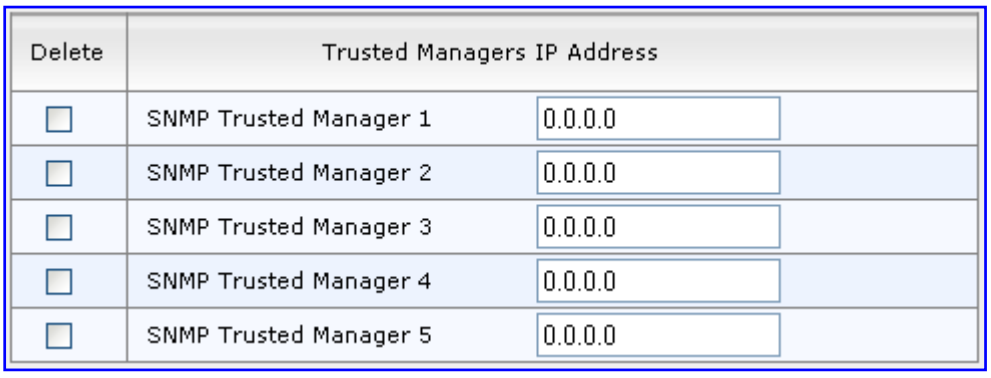
3.3.1.6.6.3 Configuring SNMP Trusted Managers

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.

➢ **To configure SNMP Trusted Managers:**

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

Figure 3-47: SNMP Trusted Managers



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 the **Submit** button to apply your changes.
5. To save the changes, see "Saving Configuration" on page 169.

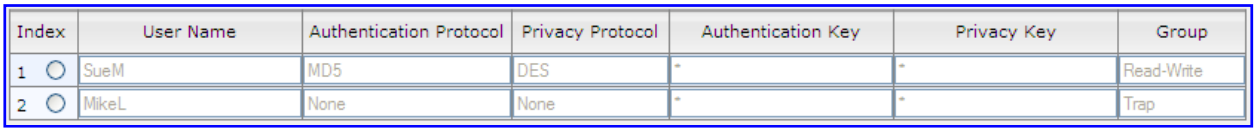
3.3.1.6.6.4 Configuring SNMP V3 Users

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

➢ **To configure the SNMP v3 users:**

1. Open the 'SNMP v3 Users' page (**Maintenance** tab > **System** menu > **Management** submenu > **SNMP** submenu > **SNMP V3 Users**).

Figure 3-48: SNMP V3 Setting Page



2. To add an SNMP v3 user, in the 'Add Index' field, enter the desired row index, and then click **Add Index**. A new row appears.
3. Configure the SNMP V3 Setting 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 169.

Notes:

- For a description of the web interface's table command buttons (e.g., **Duplicate** and **Delete**), see "Working with Tables" on page 39.
- You can also configure SNMP v3 users using the *ini* file table parameter SNMPUsers (see "SNMP Parameters" on page 366).

Table 3-9: SNMP V3 Users Parameters

Parameter	Description
Index **[SNMPUsers_Index]**	The table index. The valid range is 0 to 9.
User Name **[SNMPUsers_Username]**	Name of the SNMP v3 user. This name must be unique.
Authentication Protocol **[SNMPUsers_AuthProtocol]**	Authentication protocol of the SNMP v3 user. ▪ **[0]** None (default) ▪ **[1]** MD5 ▪ **[2]** SHA-1
Privacy Protocol **[SNMPUsers_PrivProtocol]**	Privacy protocol of the SNMP v3 user. ▪ **[0]** None (default) ▪ **[1]** DES ▪ **[2]** 3DES ▪ **[3]** AES-128 ▪ **[4]** AES-192 ▪ **[5]** AES-256
Authentication Key **[SNMPUsers_AuthKey]**	Authentication key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.

Parameter	Description
Privacy Key **[SNMPUsers_PrivKey]**	Privacy key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
Group **[SNMPUsers_Group]**	The group with which the SNMP v3 user is associated. ▪ **[0]** Read-Only (default) ▪ **[1]** Read-Write ▪ **[2]** Trap **Note:** All groups can be used to send traps.

3.3.2 VoIP Settings

The VoIP menu includes the following main submenus:

- Network (see "Network" on page 78)
- Security (see "Security" on page 89)
- Media (see "Media" on page 98)
- Applications Enabling (see "Enabling Applications" on page 102)
- Control Network (see "Control Network" on page 103)
- SIP Definitions (see "SIP Definitions" on page 110)
- Coders And Profiles (see "Coders and Profiles" on page 117)
- GW and IP to IP (see "GW and IP to IP" on page 124)
- SAS (see "SAS" on page 161)

3.3.2.1 Network

The **Network Settings** submenu includes the following items:

- IP Settings (see "Configuring IP Interface Settings" on page 78)
- IP Routing Table (see "Configuring the IP Routing Table" on page 82)
- QoS Settings (see "Configuring QoS Settings" on page 84)
- DNS (see "DNS" on page 86)

3.3.2.1.1 Configuring IP Interface Settings

The 'Multiple Interface Table' page allows you to configure up to 16 (up to 15 Control/Media interfaces and a single OAMP interface) logical network interfaces. Each interface can be defined with its own IP address, unique VLAN ID, arbitrary interface name, default gateway, and one of the following application types permitted 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)

This page also provides VLAN-related parameters for enabling VLANs and defining the 'Native' VLAN ID (i.e., VLAN ID to which incoming, untagged packets are assigned). For assigning VLAN priorities and Differentiated Services (DiffServ) for the supported Class of Service (CoS), see "Configuring the QoS Settings" on page 84.

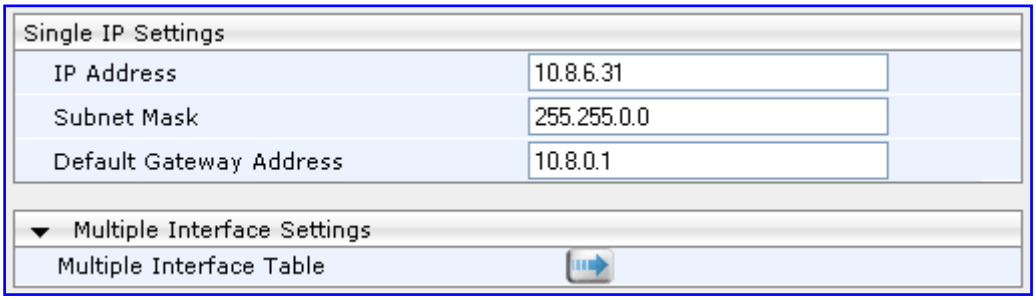
Notes:

- For a detailed description and examples of network interfaces configuration, see "Network Configuration" on page 316.
- When adding more than one interface, ensure that you enable VLANs using the 'VLAN Mode' (VlANMode) parameter.
- When booting using BootP/DHCP protocols (see the Product Reference Manual), an IP address is obtained from the server. This address is used as the OAMP address for this session, overriding the IP address you configured in the 'Multiple Interface Table' page. The address specified in this table takes effect only after you save the configuration to the device's flash memory. This enables the device to use a temporary IP address for initial management and configuration, while retaining the address (defined in this table) for deployment.
- You can define firewall rules (access list) to deny (block) or permit (allow) packets received from a specific IP interface configured in this table. These rules are configured using the AccessList parameter (see Configuring the Access List).
- You can view currently active configured IP interfaces in the 'IP Active Interfaces' page (see "Viewing Active IP Interfaces" on page 184).
- You can also configure this table using the *ini* file table parameter InterfaceTable (see "Networking Parameters" on page 333).
- For an explanation on configuring Web interface tables, see "Working with Tables" on page 39.

➢ **To configure IP network interfaces:**

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

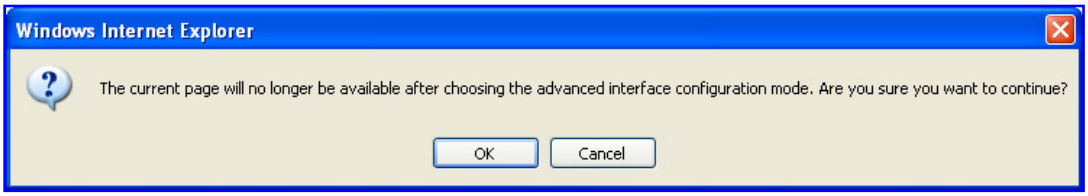
Figure 3-49: IP Settings Page



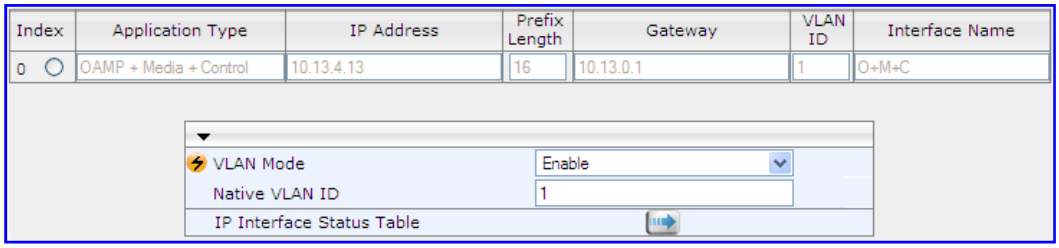
Note: The IP Settings page appears only on initial configuration (i.e., IP interfaces have never been configured) or after the device is restored to default settings. If you have already configured IP interfaces, then the Multiple Interface Table page appears instead, as shown in Step 3.

2. Under the 'Multiple Interface Settings' group, click the **Multiple Interface Table** button; a confirmation message box appears:

Figure 3-50: Confirmation Message for Accessing the Multiple Interface Table



3. Click **OK** to confirm; the 'Multiple Interface Table' page appears:



4. 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.
5. Configure the interface according to the table below.
6. Click the **Apply** button; the interface is added to the table and the **Done** button appears.
7. 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 323), a warning message is displayed.
8. Save the changes to flash memory and reset the device (see "Saving Configuration" on page 169).

To view network interfaces that are currently active, click the **IP Interface Status Table** button. For a description of this display, see "Viewing Active IP Interfaces" on page 184.

Table 3-10: Multiple Interface Table Parameters Description

Parameter	Description
Table parameters	
Index	Index of each interface. The range is 0 to 15.
Web: Application Type EMS: Application Types **[InterfaceTable_ApplicationTypes]**	Types of applications that are allowed on the specific interface. ▪ **[0]** OAMP = Only Operations, Administration, Maintenance and Provisioning (OAMP) applications (e.g., Web, Telnet, SSH, and SNMP) are allowed on the interface. ▪ **[1]** Media = Only Media (i.e., RTP streams of voice) is allowed on the interface. ▪ **[2]** Control = Only Call Control applications (e.g., SIP) are allowed on the interface. ▪ **[3]** OAMP + Media = Only OAMP and Media applications are allowed on the interface. ▪ **[4]** OAMP + Control = Only OAMP and Call Control applications are allowed on the interface.

Parameter	Description
	▪ **[5]** Media + Control = Only Media and Call Control applications are allowed on the interface. ▪ **[6]** OAMP + Media + Control = All application types are allowed on the interface. **Notes:** ▪ A single OAMP interface (and only one) must be configured. This OAMP interface can be combined with Media and Control interfaces. ▪ At least one interface for Media traffic and at least one interface for Control traffic must be configured. These interfaces can be combined (i.e., Media + Control, or OAMP + Media + Control). ▪ Multiple interfaces for Media, Control, and Media and Control can be configured. ▪ At least one IPv4 interface with Control must be configured. This can be combined with OAMP and Media. ▪ At least one IPv4 interface with Media must be configured. This can be combined with OAMP and Control.
Web/EMS: IP Address **[InterfaceTable_IPAddres]**	The IPv4 IP address in dotted-decimal notation. **Notes:** ▪ Each interface must be assigned a unique IP address. ▪ When booting using BootP/DHCP protocols, an IP address is obtained from the server. This address is used as the OAMP address for the initial session, overriding the address configured using the InterfaceTable. The address configured for OAMP applications in this table becomes available when booting from flash again. This enables the device to operate with a temporary address for initial management and configuration while retaining the address to be used for deployment.
Web/EMS: Prefix Length **[InterfaceTable_PrefixLength]**	Defines the 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 (e.g. 192.168.0.0/16 is synonymous with 192.168.0.0 and a subnet of 255.255.0.0. Defines 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 (refer to http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing for more information). For IPv4 Interfaces, the prefix length values range from 0 to 31. **Note:** Subnets of different interfaces must not overlap in any

Parameter	Description
	way (e.g., defining two interfaces with 10.0.0.1/8 and 10.50.10.1/24 is invalid). Each interface must have its own address space.
Web/EMS: Gateway **[InterfaceTable_Gateway]**	Defines the IP address of the default gateway for this interface. **Notes:** ▪ A default gateway can be defined for each interface. ▪ The default gateway's IP address must be in the same subnet as the interface address.
Web/EMS: VLAN ID **[InterfaceTable_VlanID]**	Defines the VLAN ID for each interface. Incoming traffic with this VLAN ID is routed to the corresponding interface and outgoing traffic from that interface is tagged with this VLAN ID. **Notes:** ▪ The VLAN ID must be unique for each interface. ▪ VLANs are available only when booting the device from flash. When booting using BootP/DHCP protocols, VLANs are disabled to allow easier maintenance access. In this scenario, multiple network interface capabilities are not available.
Web/EMS: Interface Name **[InterfaceTable_InterfaceName]**	Defines a string (up to 16 characters) to name this interface. This name is displayed in management interfaces (Web, CLI and SNMP) for clarity (and has no functional use), as well as in the 'SIP Media Realm' and 'SIP Interface' tables. **Notes:** ▪ This parameter is mandatory. ▪ The name must be unique for each interface.
General Parameters	
VLAN Mode **[VlanMode]**	For a description of this parameter, see Networking Parameters on page 333.
Native VLAN ID **[VLANNativeVlanID]**	For a description of this parameter, see Networking Parameters on page 333.

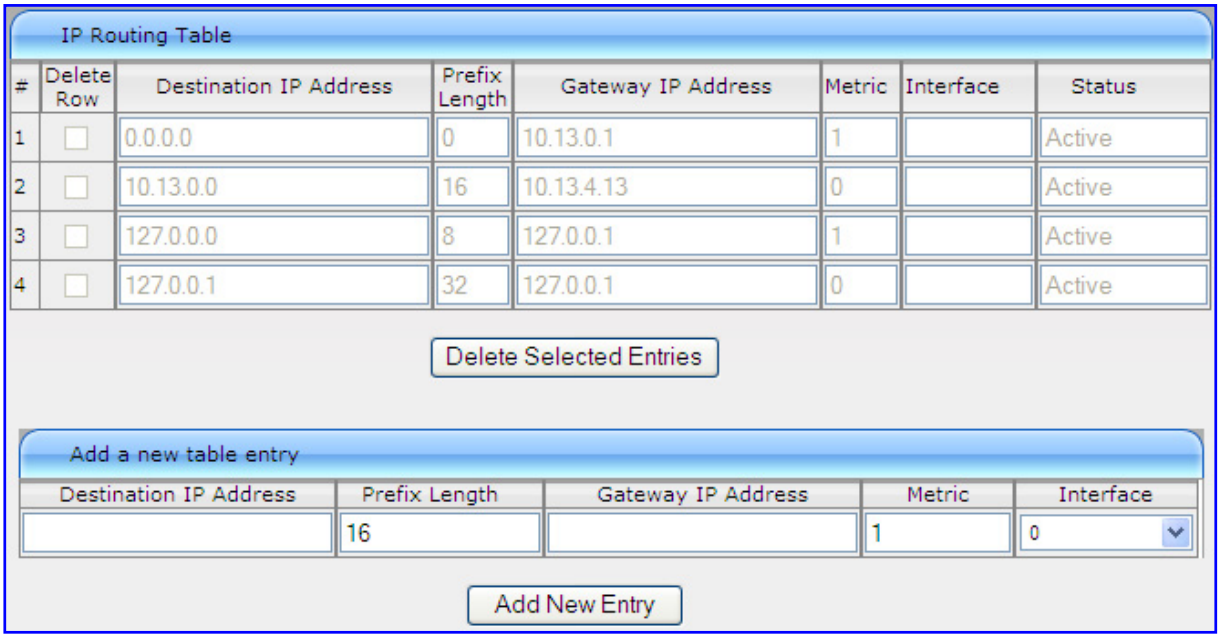
3.3.2.1.2 Configuring the IP Routing Table

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. Before sending an IP packet, the device searches this table for an entry that matches the requested destination host/network. If such an entry is found, the device sends the packet to the indicated router. If no explicit entry is found, the packet is sent to the default gateway (see Configuring IP Interface Settings on page 78).

➢ **To configure static IP routing:**

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

Figure 3-51: IP Routing Table Page



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.
- You can also configure the IP Routing table using the *ini* file table parameter StaticRouteTable.

Table 3-11: IP Routing Table Description

Parameter	Description
Destination IP Address **[StaticRouteTable_Destination]**	Specifies the IP address of the destination host/network.
Prefix Length **[StaticRouteTable_PrefixLength]**	Specifies the subnet mask of the destination host/network.
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 'Destination Mask'. For example, to reach the network 10.8.x.x, enter 10.8.0.0 in the field 'Destination IP Address' and 255.255.0.0 in the field 'Destination Mask'. As a result of the AND operation, the value of the last two octets in the field 'Destination IP Address' is ignored. To reach a specific host, enter its IP address in the field 'Destination IP Address' and 255.255.255.255 in the field 'Destination Mask'.	

Parameter	Description
Gateway IP Address **[StaticRouteTable_Gateway]**	The IP address of the router (next hop) to which the packets are sent if their destination matches the rules in the adjacent columns. **Note:** 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	The number of hops needed to get to the specified destination. **Note:** 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 **[StaticRouteTable_InterfaceName]**	Associates this routing rule with a network interface. This value is the index of the network interface as defined in the Multiple Interface table (see "Configuring IP Interface Settings" on page 78). **Note:** 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: ▪ "Active" - routing rule is used ny the device ▪ "Inactive" - routing rule is not applied

3.3.2.1.3 Configuring QoS Settings

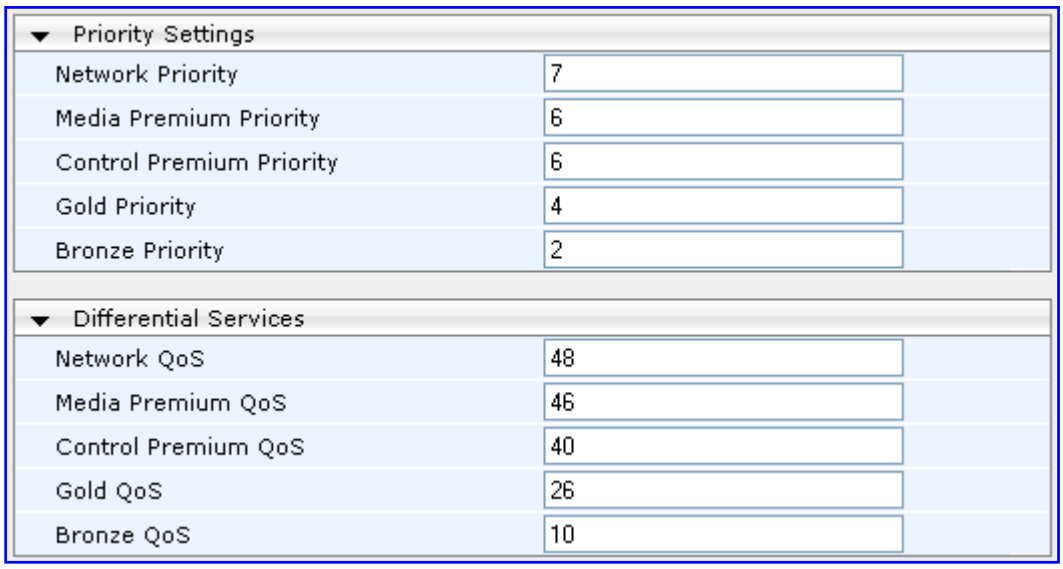
The 'QoS Settings' page is used for configuring the Layer-2 and Layer-3 Quality of Service (QoS) parameters. DiffServ is an architecture providing different types or levels of service for IP traffic. DiffServ (according to RFC 2474), prioritizes certain traffic types based on their priority, thereby, 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.

This page allows you to assign different VLAN priorities (IEEE 802.1p) and Differentiated Services (DiffServ) to the supported Class of Service (CoS) - Network, Media Premium, Control Premium, Gold, and Bronze. For a detailed description of the parameters appearing on this page, see "Networking Parameters" on page 333. For a description on QoS and the mapping of each application to a class of service, see "Quality of Service Parameters" on page 320.

➢ **To configure QoS:**

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

Figure 3-52: QoS Settings Page



2. Configure the QoS parameters as required.
3. Click the **Submit** button to save your changes.
4. Save the changes to flash memory (see "Saving Configuration" on page 169).

3.3.2.1.4 DNS

The **DNS** submenu includes the following items:

- DNS Settings (refer to "Configuring DNS Settings" on page 86)
- Internal DNS Table (refer to "Configuring the Internal DNS Table" on page 87)
- Internal SRV Table (refer to "Configuring the Internal SRV Table" on page 88)

3.3.2.1.4.1 Configuring DNS Settings

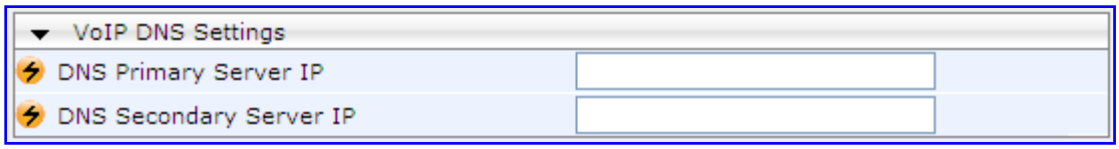
The 'DNS Settings' page defines the VoIP Domain Name System (DNS) server IP addresses.

Note: For a detailed description of the DNS parameters, refer to "DNS Parameters" on page 342.

➢ **To define the DNS server:**

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

Figure 3-53: DNS Settings Page



2. In the 'DNS Primary Server IP' field, enter the IP address of the primary DNS server (in dotted-decimal notation, for example, 10.8.2.255).
3. Optionally, in the 'DNS Secondary Server IP', enter the IP address of the second DNS server (in dotted-decimal notation).
4. Click the **Submit** button to apply your changes.
5. Save the changes to flash memory (refer to "Saving Configuration" on page 169).

3.3.2.1.4.2 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 (e.g., when using the 'Tel to IP Routing' for Tel-to-IP call routing). Up to four different IP addresses can be assigned to the same host name (typically used for alternative Tel-to-IP call routing).

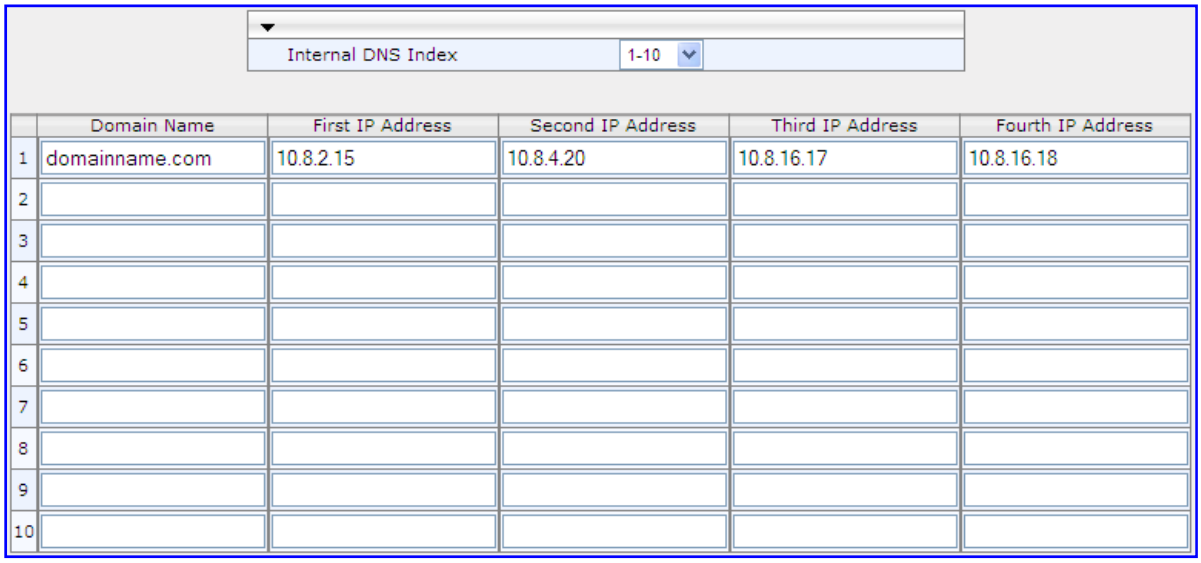
Notes:

- The device initially attempts to resolve a domain name using the Internal DNS table. If the domain name isn't listed in the table, the device performs a DNS resolution using an external DNS server (defined in "Configuring DNS Settings" on page 86).
- You can also configure the DNS table using the *ini* file table parameter DNS2IP (see "DNS Parameters" on page 342).

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

1. Open the 'Internal DNS Table' page (**Configuration** tab > **VoIP** menu > **Network** submenu > **DNS** submenu > **Internal DNS Table**).

Figure 3-54: Internal DNS Table Page



2. In the 'Domain Name' field, enter the host name to be translated. You can enter a string of up to 31 characters.
3. In the 'First IP Address' field, enter the first IP address (in dotted-decimal format notation) to which the host name is translated.
4. Optionally, in the 'Second IP Address', 'Third IP Address', and 'Second IP Address' fields, enter the next IP addresses to which the host name is translated.
5. Click the **Submit** button to save your changes.
6. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.1.4.3 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. 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 an Service Record (SRV) resolution using an external DNS server (defined in "Configuring DNS Settings" on page 86).
- You can also configure the Internal SRV table using the *ini* file table parameter SRV2IP (see "DNS Parameters" on page 342).

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

1. Open the 'Internal SRV Table' page (**Configuration** tab > **VoIP** menu > **Network** submenu > **DNS** submenu > **Internal SRV Table**).

Figure 3-55: Internal SRV Table Page

	Domain Name	Transport Type	DNS Name 1	Priority	Weight	Port	DNS Name 2	Priority	Weight	Port	DNS Name 3	Priority	Weight	Port
1		UDP												
2		UDP												
3		UDP												
4		UDP												
5		UDP												
6		UDP												
7		UDP												
8		UDP												
9		UDP												
10		UDP												

2. In the 'Domain Name' field, enter the host name to be translated. You can enter a string of up to 31 characters.
3. From the 'Transport Type' drop-down list, select a transport type.
4. In the 'DNS Name 1' field, enter the first DNS A-Record to which the host name is translated.
5. In the 'Priority', 'Weight' and 'Port' fields, enter the relevant values
6. Repeat steps 4 through 5, for the second and third DNS names, if required.
7. Repeat steps 2 through 6, for each entry.
8. Click the **Submit** button to save your changes.
9. To save the changes so they are available after a hardware reset or power fail, see "Saving Configuration" on page 169.

3.3.2.2 Security

The **Security Settings** submenu allows you to configure various security settings. This menu contains the following page items:

- Firewall Settings (see "Configuring Firewall Settings" on page 89)
- 802.1x Settings (see "Configuring 802.1x Settings" on page 92)
- General Security Settings (see "Configuring General Security Settings" on page 93)
- IPSec Proposal Table (see "Configuring IP Security Associations Table" on page 95)
- IPSec Association Table (see "Configuring IP Security Proposal Table" on page 94)

3.3.2.2.1 Configuring Firewall Settings

The device provides an internal firewall, allowing you (the security administrator) to define network traffic filtering rules. You can add up to 50 ordered firewall rules.

The access list provides the following firewall rules:

- Block traffic from known malicious sources
- Only allow traffic from known friendly sources, and block all others
- Mix allowed and blocked network sources
- Limit traffic to a pre-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 the top down until a matching rule is found. This rule can either deny (*block*) or permit (*allow*) 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. For detailed information on the internal firewall, refer to the *Product Reference Manual*.

Notes:

- It is recommended to add a rule at the end of your table that blocks all traffic and add firewall rules above it (in the table) that allow traffic (with bandwidth limitations). To block all traffic, the following must be set:
  - IP address to 0.0.0.0
  - Prefix length of 0 (implies the rule can match any IP address)
  - Local port range 0-65535
  - Protocol "Any"
  - Action Upon Match "block"
- You can also configure the firewall settings using the *ini* file table parameter AccessList (see "Security Parameters" on page 356).

➢ **To add firewall rules:**

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

Figure 3-56: Firewall Settings Page

Edit Rule	Rule Status	Source IP	Prefix Length	Local Port Range	Protocol	Use Specific Interface	Interface Name	Packet Size	Byte rate	Burst Bytes	Action Upon Match	Match Count
1	Active	mgmt.customer.com	32	0 - 80	tcp	Enable	O+M+C	0	0	0	Allow	0
2	Active	192.0.0.0	8	0-65535	Any	Disable	None	0	40000	50000	ALLOW	0
3	Active	10.31.4.0	24	4000-9000	Any	Disable	None	0	0	0	BLOCK	0
4	Active	10.4.0.0	16	4000-9000	Any	Disable	None	0	0	0	BLOCK	0

2. In the 'Add' field, enter the index of the access rule that you want to add, and then click **Add**; a new firewall rule index appears in the table.
3. Configure the firewall rule's parameters according to the table below.
4. Click one of the following buttons:
   - **Apply:** saves the new rule (without activating it).
   - **Duplicate Rule:** adds a new rule by copying a selected rule.
   - **Activate:** saves the new rule and activates it.
   - **Delete:** deletes the selected rule.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.

The previous figure shows the following access list settings:

- **Rule #1:** traffic from the host 'mgmt.customer.com' destined to TCP ports 0 to 80, is always allowed.
- **Rule #2:** traffic from the 192.xxx.yyy.zzz subnet, is limited to a rate of 40 Kbytes per second (with an allowed burst of 50 Kbytes). Note that the rate is specified in bytes, not bits, per second; a rate of 40000 bytes per second, nominally corresponds to 320 kbps.
- **Rule #3:** traffic from the subnet 10.31.4.xxx destined to ports 4000-9000 is always blocked, regardless of protocol.
- **Rule #4:** traffic from the subnet 10.4.xxx.yyy destined to ports 4000-9000 is always blocked, regardless of protocol.
- All other traffic is allowed

➢ **To edit a rule:**

1. In the 'Edit Rule' column, select the rule that you want to edit.
2. Modify the fields as desired.
3. Click the **Apply** button to save the changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

➢ **To activate a de-activated rule:**

1. In the 'Edit Rule' column, select the de-activated rule that you want to activate.
2. Click the **Activate** button; the rule is activated.

➢ **To de-activate an activated rule:**

1. In the 'Edit Rule' column, select the activated rule that you want to de-activate.
2. Click the **DeActivate** button; the rule is de-activated.

➢ **To delete a rule:**

1. Select the radio button of the entry you want to activate.
2. Click the **Delete Rule** button; the rule is deleted.
3. To save the changes to flash memory, see "Saving Configuration" on page 169.

Table 3-12: Internal Firewall Parameters

Parameter	Description
Rule Status	A read-only field indicating whether the rule is active or not. **Note:** After device reset, all rules are active.
Source IP **[AccessList_Source_IP]**	IP address (or DNS name) or a specific host name of the source network (i.e., from where the incoming packet is received).
Prefix Length **[AccessList_PrefixLen]**	IP network mask. 32 for a single host, or the appropriate value for the source IP addresses. ▪ A value of 8 corresponds to IPv4 subnet class A (network mask of 255.0.0.0). ▪ A value of 16 corresponds to IPv4 subnet class B (network mask of 255.255.0.0). ▪ A value of 24 corresponds to IPv4 subnet class C (network mask of 255.255.255.0). The IP address of the sender of the incoming packet is trimmed in accordance with the prefix length (in bits) and then compared to the parameter 'Source IP'.
Local Port Range **[AccessList_Start_Port]** **[AccessList_End_Port]**	The destination UDP/TCP ports (on this device) to which packets are sent. The valid range is 0 to 65535. **Note:** When the protocol type isn't TCP or UDP, the entire range must be provided.
Protocol **[AccessList_Protocol]**	The protocol type (e.g., UDP, TCP, ICMP, ESP or 'Any'), or the IANA protocol number (in the range of 0 (Any) to 255). **Note:** 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 **[AccessList_Use_Specific_Interface]**	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): ▪ **[0]** Disable (default) ▪ **[1]** Enable **Notes:** ▪ If enabled, then in the 'Interface Name' field (described below), select the interface to which the rule is applied. ▪ If disabled, then the rule applies to all interfaces.
Interface Name **[AccessList_Interface_ID]**	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 (see "Configuring IP Interface Settings" on page 78).

Parameter	Description
Packet Size **[AccessList_Packet_Size]**	Maximum allowed packet size. The valid range is 0 to 65535. **Note:** When filtering fragmented IP packets, this field relates to the overall (re-assembled) packet size, and not to the size of each fragment.
Byte Rate **[AccessList_Byte_Rate]**	Expected traffic rate (bytes per second). This field defines 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 **[AccessList_Byte_Burst]**	Tolerance of traffic rate limits (number of bytes).
Action Upon Match **[AccessList_Allow_Type]**	Action upon match (i.e., 'Allow' or 'Block').
Match Count **[AccessList_MatchCount]**	A read-only field displaying the number of packets accepted/rejected by the specific rule.

3.3.2.2.2 Configuring 802.1x Settings

The '802.1x Settings' page is used to configure IEEE 802.1X LAN security. The device can function as an IEEE 802.1X supplicant. IEEE 802.1X is a standard for port-level security on secure Ethernet switches; when a device is connected to a secure port, no traffic is allowed until the identity of the device is authenticated.

The device supports the following Extensible Authentication Protocol (EAP) variants:

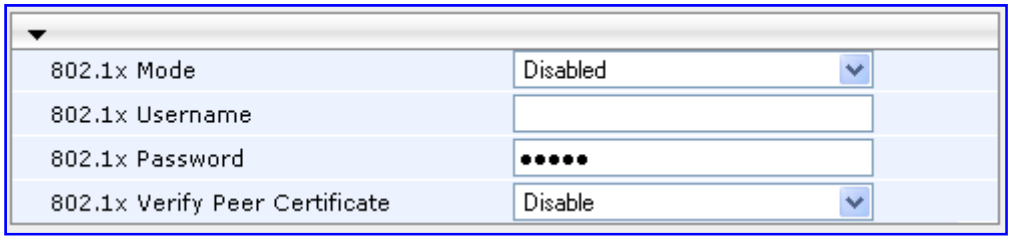
- MD5-Challenge (EAP-MD5)
- Protected EAP (PEAPv0 with EAP-MSCHAPv2)
- EAP-TLS

For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333. For a detailed description of this feature, refer to the *Product Reference Manual*.

➢ **To configure the 802.1x parameters:**

1. Open the '802.1x Settings' page (**Configuration** tab > **VoIP** menu > **Security** submenu > **802.1x Settings**).

Figure 3-57: 8021x Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

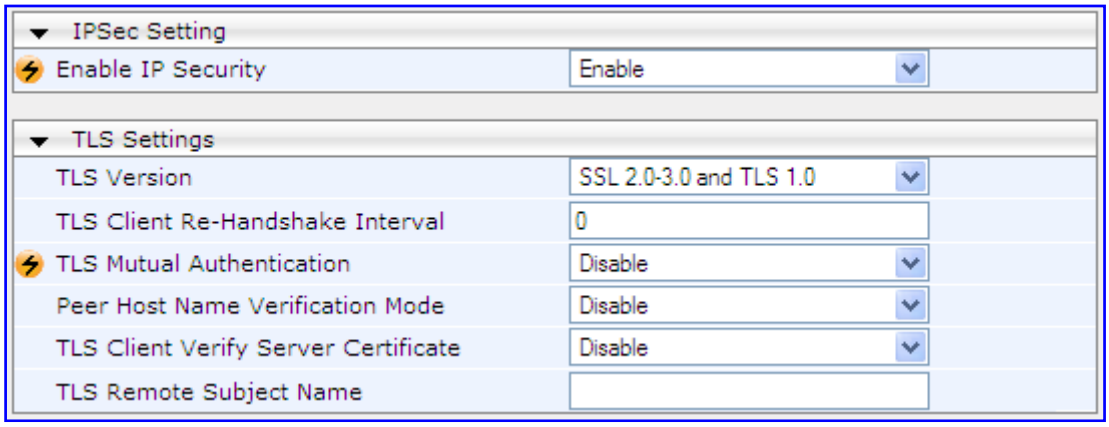
3.3.2.2.3 Configuring General Security Settings

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 333.

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

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

Figure 3-58: General Security Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 169.

3.3.2.2.4 Configuring IP Security Proposal Table

The 'IP Security Proposals Table' page is used to configure Internet Key Exchange (IKE) with up to four proposal settings. Each proposal defines an encryption algorithm, an authentication algorithm, and a Diffie-Hellman group identifier. The same set of proposals applies to both Main mode and Quick mode.

Note: You can also configure the IP Security Proposals table using the *ini* file table parameter IPsecProposalTable (see "Security Parameters" on page 356).

➢ **To configure IP Security Proposals:**

1. Open the 'IP Security Proposals Table' page (**Configuration** tab > **VoIP** menu > **Security** submenu > **IPSec Proposal Table**).

Figure 3-59: IP Security Proposals Table

Index	Encryption Algorithm	Authentication Algorithm	Diffie Hellman Group
0	3DES CBC	HMAC SHA1 96	Group 2 [1024 Bits]
1	3DES CBC	HMAC MD5 96	Group 2 [1024 Bits]
2	DES CBC	HMAC SHA1 96	Group 1 [768 Bits]
3	DES CBC	HMAC MD5 96	Group 1 [768 Bits]

In the figure above, four proposals are defined.

2. Select an Index, click **Edit**, and then modify the proposal as required.
3. Click **Apply**.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

To delete a proposal, select the relevant Index number, and then click **Delete**.

Table 3-13: IP Security Proposals Table Configuration Parameters

Parameter Name	Description
Encryption Algorithm **[IPsecProposalTable_EncryptionAlgorithm]**	Determines the encryption (privacy) algorithm. ▪ **[0]** NONE ▪ **[1]** DES CBC ▪ **[2]** 3DES CBC ▪ **[3]** AES (default)
Authentication Algorithm **[IPsecProposalTable_AuthenticationAlgorithm]**	Determines the message authentication (integrity) algorithm. ▪ **[0]** NONE ▪ **[2]** HMAC SHA1 96 ▪ **[4]** HMAC MD5 96 (default)
Diffie Hellman Group **[IPsecProposalTable_DHGroup]**	Determines the length of the key created by the DH protocol for up to four proposals. For the *ini* file parameter, *X* depicts the proposal number (0 to 3). ▪ **[0]** Group 1 (768 Bits) = DH-786-Bit ▪ **[1]** Group 2 (1024 Bits) (default) = DH-1024-Bit

If no proposals are defined, the default settings (shown in the following table) are applied.

Table 3-14: Default IPSec/IKE Proposals

Proposal	Encryption	Authentication	DH Group
Proposal 0	3DES	SHA1	Group 2 (1024 bit)
Proposal 1	3DES	MD5	Group 2 (1024 bit)
Proposal 2	3DES	SHA1	Group 1 (786 bit)
Proposal 3	3DES	MD5	Group 1 (786 bit)

3.3.2.2.5 Configuring IP Security Associations Table

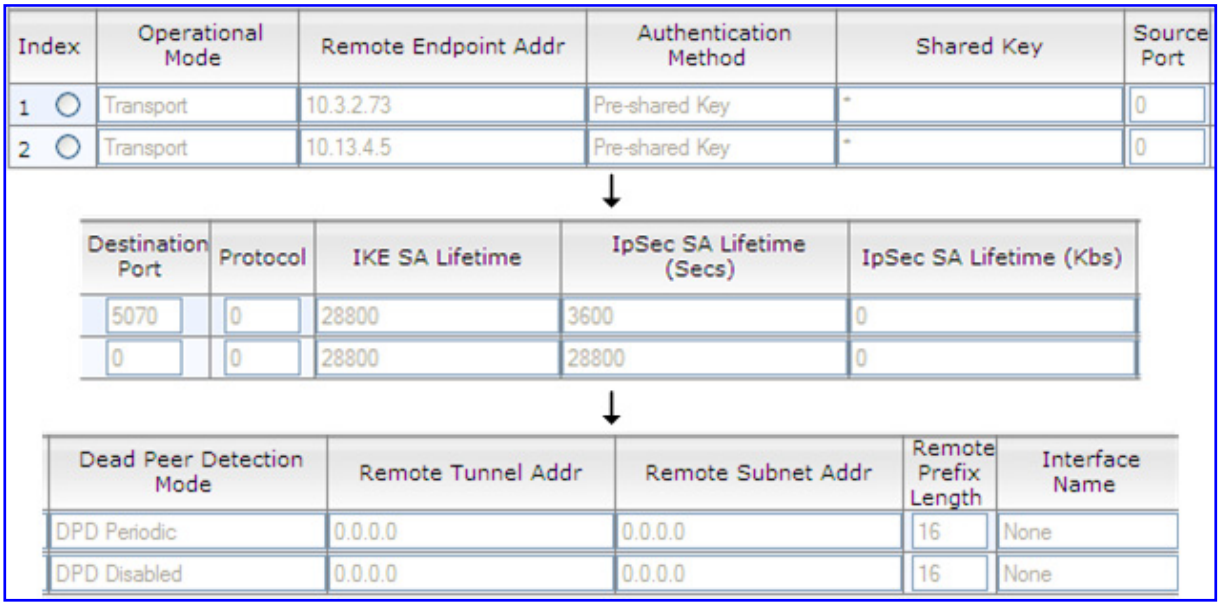
The 'IP Security Associations Table' page allows you to configure up to 20 peers (hosts or networks) for IP security (IPSec)/IKE. Each of the entries in the IPSec Security Association table controls both Main Mode and Quick Mode configuration for a single peer

Note: You can also configure the IP Security Associations table using the *ini* file table parameter IPsecSATable (see "Security Parameters" on page 356).

➢ **To configure the IPSec Association table:**

1. Open the 'IP Security Associations Table' page (**Configuration** tab > **VoIP** menu > **Security** submenu > **IPSec Association Table**). (Due to the length of the table, the figure below shows sections of this table.)

Figure 3-60: IP Security Associations Table Page



2. Add an Index or select the Index rule you want to edit.
3. Configure the rule according to the table below.
4. Click **Apply**; the rule is applied on-the-fly.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.

Table 3-15: IP Security Associations Table Configuration Parameters

Parameter Name	Description
Operational Mode **[IPsecSATable_IPsecMode]**	Defines the IPSec mode of operation. ▪ **[0]** Transport (default) ▪ **[1]** Tunnel
Remote Endpoint Addr **[IPsecSATable_RemoteEndpointAddressOrName]**	Defines the IP address or DNS host name of the peer. **Note:** This parameter is applicable only if the Operational Mode is set to Transport.
Authentication Method **[IPsecSATable_AuthenticationMethod]**	Selects the method used for peer authentication during IKE main mode. ▪ **[0]** Pre-shared Key (default) ▪ **[1]** RSA Signature = in X.509 certificate **Note:** For RSA-based authentication, both peers must be provisioned with certificates signed by a common CA. For more information on certificates see "Server Certificate Replacement" on page 62.
Shared Key **[IPsecSATable_SharedKey]**	Defines the pre-shared key (in textual format). Both peers must use the same pre-shared key for the authentication process to succeed. **Notes:** ▪ This parameter is applicable only if the Authentication Method parameter is set to pre-shared key. ▪ The pre-shared key forms the basis of IPSec security and therefore, it should be handled with care (the same as sensitive passwords). It is not recommended to use the same pre-shared key for several connections. ▪ Since the *ini* file is plain text, loading it to the device over a secure network connection is recommended. Use a secure transport such as HTTPS, or a direct crossed-cable connection from a management PC. ▪ After it is configured, the value of the pre-shared key cannot be retrieved.
Source Port **[IPsecSATable_SourcePort]**	Defines the source port to which this configuration applies. The default value is 0 (i.e., any port).
Destination Port **[IPsecSATable_DestPort]**	Defines the destination port to which this configuration applies. The default value is 0 (i.e., any port).
Protocol **[IPsecSATable_Protocol]**	Defines the protocol type to which this configuration applies. Standard IP protocol numbers, as defined by the Internet Assigned Numbers Authority (IANA) should be used, for example: ▪ 0 = Any protocol (default) ▪ 17 = UDP ▪ 6 = TCP
IKE SA Lifetime **[IPsecSATable_Phase1SaLifetimeInSec]**	Determines the duration (in seconds) for which the negotiated IKE SA (Main mode) is valid. After this time expires, the SA is re-negotiated.

Parameter Name	Description
	Note: Main mode negotiation is a processor-intensive operation; for best performance, do not set this parameter to less than 28,800 (i.e., eight hours). The default value is 0 (i.e., unlimited).
IPSec SA Lifetime (sec) **[IPsecSATable_Phase2SaLifetimeInSec]**	Determines the duration (in seconds) for which the negotiated IPSec SA (Quick mode) is valid. After this time expires, the SA is re-negotiated. The default value is 0 (i.e., unlimited). **Note:** For best performance, a value of 3,600 (i.e., one hour) or more is recommended.
IPSec SA Lifetime (Kbs) **[IPsecSATable_Phase2SaLifetimeInKB]**	Determines the maximum volume of traffic (in kilobytes) for which the negotiated IPSec SA (Quick mode) is valid. After this specified volume is reached, the SA is re-negotiated. The default value is 0 (i.e., the value is ignored).
Dead Peer Detection Mode **[IPsecSATable_DPDmode]**	Configures dead peer detection (DPD), according to RFC 3706. ▪ **[0]** DPD Disabled (default) ▪ **[1]** DPD Periodic = DPD is enabled with message exchanges at regular intervals ▪ **[2]** DPD on demand = DPD is enabled with on-demand checks - message exchanges as needed (i.e., before sending data to the peer). If the liveliness of the peer is questionable, the device sends a DPD message to query the status of the peer. If the device has no traffic to send, it never sends a DPD message. **Note:** For detailed information on DPD, refer to the P*roduct Reference Manual*.
Remote Tunnel Addr **[IPsecSATable_RemoteTunnelAddress]**	Defines the IP address of the peer router. **Note:** This parameter is applicable only if the Operational Mode is set to Tunnel.
Remote Subnet Addr **[IPsecSATable_RemoteSubnetIPAddress]**	Defines the IP address of the remote subnet. Together with the Prefix Length parameter (below), this parameter defines the network with which the IPSec tunnel allows communication. **Note:** This parameter is applicable only if the Operational Mode is set to Tunnel.
Remote Prefix Length **[IPsecSATable_RemoteSubnetPrefixLength]**	Defines the prefix length of the Remote Subnet IP Address parameter (in bits). The prefix length defines the subnet class of the remote network. A prefix length of 16 corresponds to a Class B subnet (255.255.0.0); a prefix length of 24 corresponds to a Class C subnet (255.255.255.0). **Note:** This parameter is applicable only if the Operational Mode is set to Tunnel.
Interface Name **[IPsecSATable_InterfaceName]**	Associates this IPSec rule with a network interface that is defined in the Multiple Interface table (Interface Name column) - see "Configuring IP Interface Settings" on page 78.

3.3.2.3 Media

The **Media** submenu allows you to configure the device's channel parameters and contains the following items:

- Voice Settings (see "Configuring Voice Settings" on page 98)
- Fax/Modem/CID Settings (see "Configuring Fax/Modem/CID Settings" on page 99)
- RTP/RTCP Settings (see "Configuring RTP/RTCP Settings" on page 100)
- General Media Settings (see "Configuring General Media Settings" on page 101)
- Analog Settings (see "Configuring Analog Settings" on page 101)
- Media Security (see "Configuring Media Security" on page 102)

Note: Some channel parameters can be configured per channel or call routing, using profiles (see Coders and Profile Definitions on page 117).

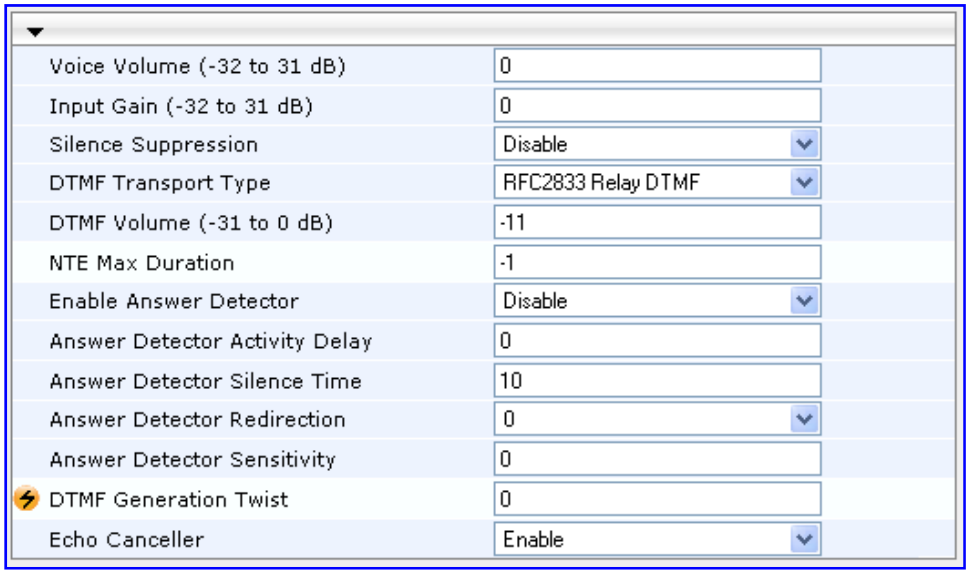
3.3.2.3.1 Configuring Voice Settings

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 333.

➢ **To configure the voice parameters:**

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

Figure 3-61: Voice Settings Page



2. Configure the Voice parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

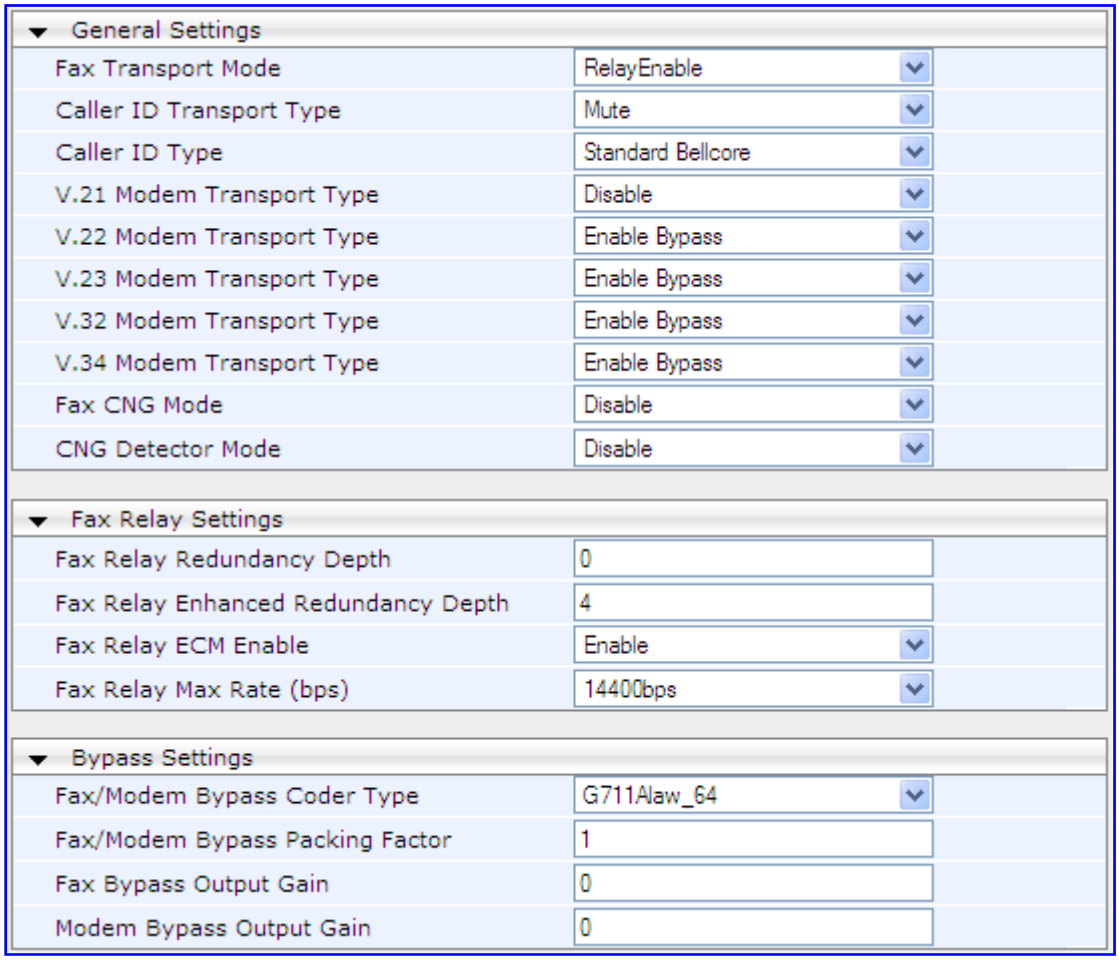
3.3.2.3.2 Configuring Fax/Modem/CID Settings

The 'Fax/Modem/CID Settings' page is used for configuring fax, modem, and Caller ID (CID) parameters. For a detailed description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333.

➢ **To configure the fax, modem, and CID parameters:**

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

Figure 3-62: Fax/Modem/CID Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

Note: Some SIP parameters override these fax and modem parameters (see the parameter IsFaxUsed, and V.152 parameters in Section "V.152 Support" on page 253).

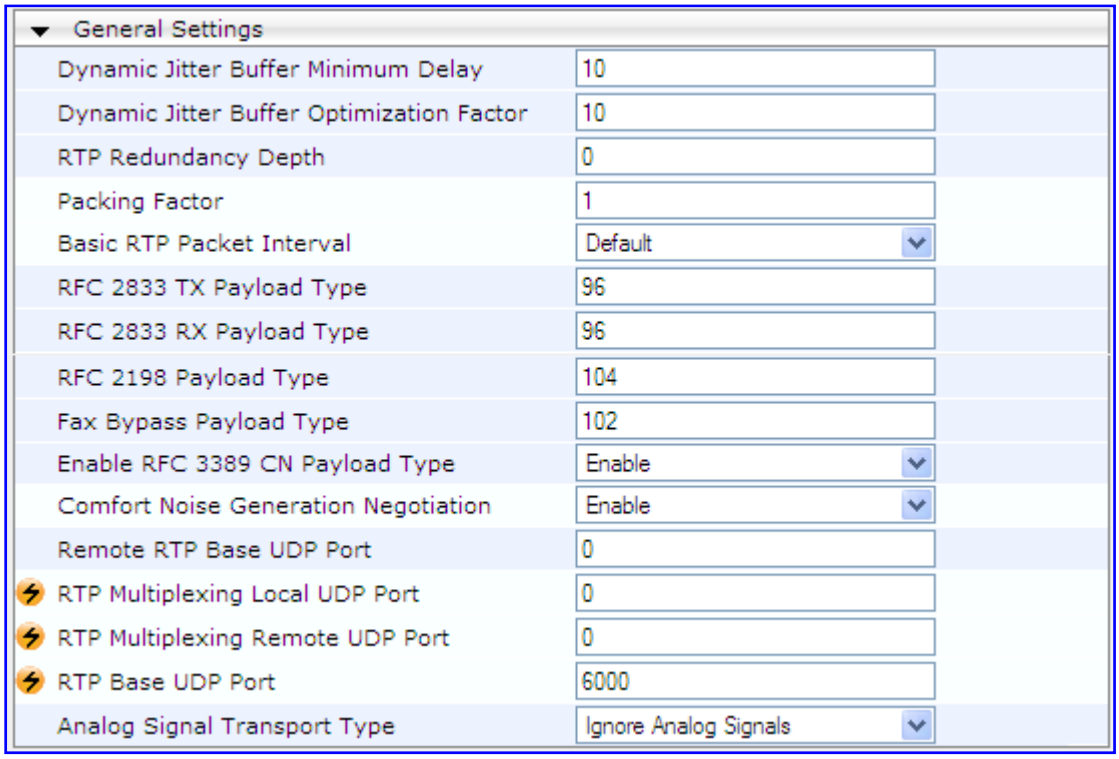
3.3.2.3.3 Configuring RTP/RTCP Settings

The 'RTP/RTCP Settings' page configures the Real-Time Transport Protocol (RTP) and Real-Time Transport (RTP) Control Protocol (RTCP) parameters. For a detailed description of the parameters appearing on this page, refer to "Configuration Parameters Reference" on page 333.

➢ **To configure the RTP/RTCP parameters:**

1. Open the 'RTP/RTCP Settings' page (**Configuration** tab > **VoIP** menu > **Media** submenu > **RTP/RTCP Settings**).

Figure 3-63: RTP/RTCP Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 169.

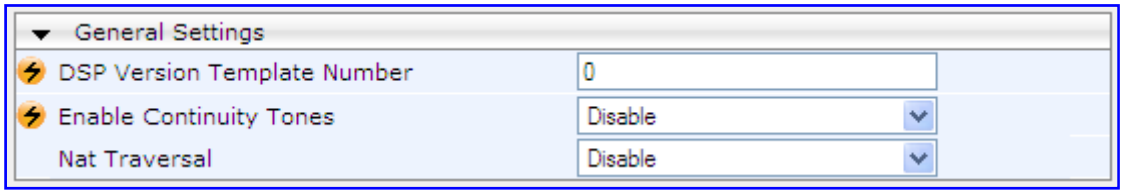
3.3.2.3.4 Configuring General Media Settings

The 'General Media Settings' page allows you to configure various media parameters. For a detailed description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333.

➢ **To configure general media parameters:**

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

Figure 3-64: General Media Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.3.5 Configuring Analog Settings

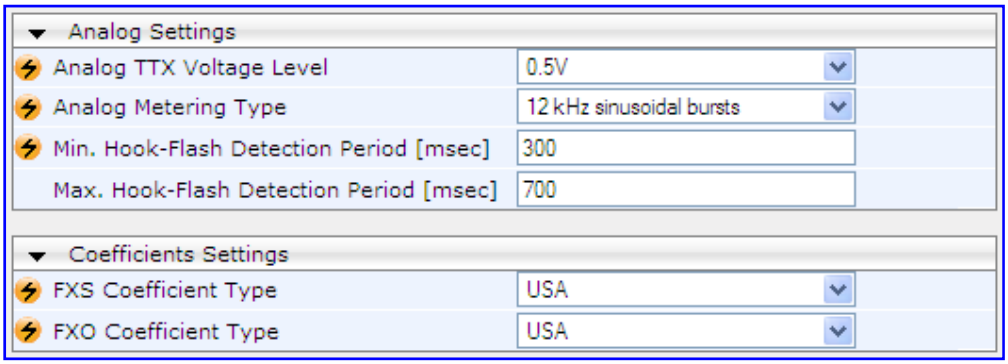
The 'Analog Settings' page allows you to configure various analog parameters. For a detailed description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333.

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 3-65: Analog Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

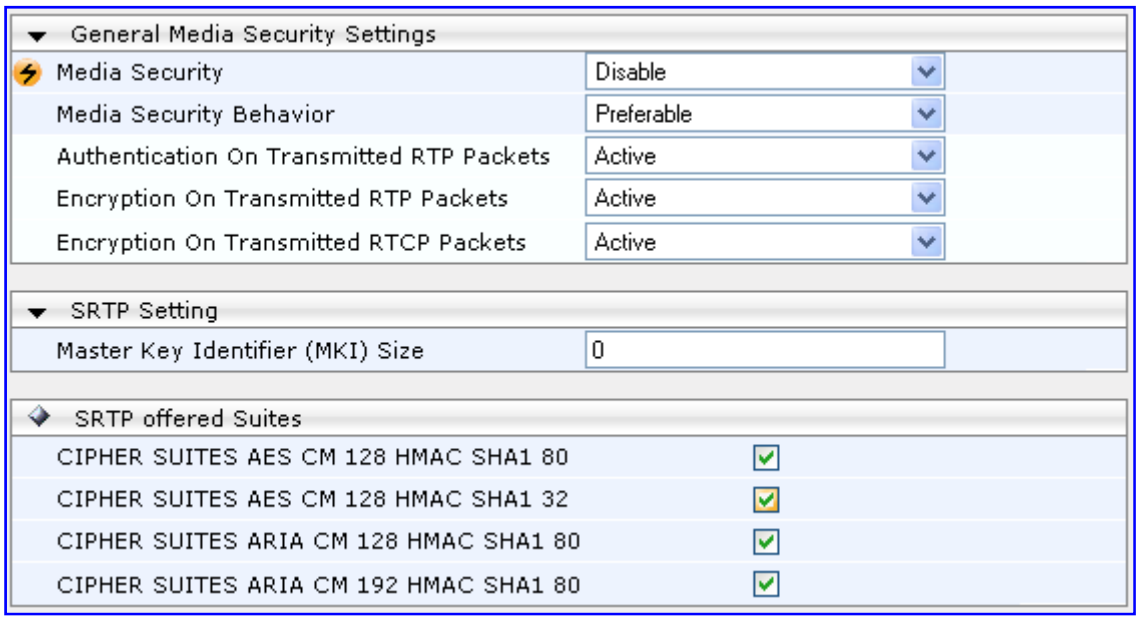
3.3.2.3.6 Configuring Media Security

The 'Media Security' page allows you to configure media security. For a detailed description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333.

➢ **To configure media security:**

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

Figure 3-66: Media Security Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.4 Applications Enabling

3.3.2.4.1 Enabling Applications

The 'Applications Enabling' page allows you to enable the following application:

- Stand-Alone Survivability (SAS) application

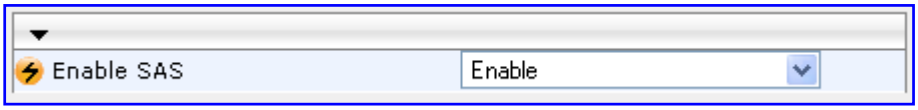
Notes:

- This page displays the application only if the device is installed with the relevant Software Upgrade Key supporting the application (see "Loading Software Upgrade Key" on page 172).
- For enabling an application, a device reset is required.

➢ **To enable an application:**

1. Open the 'Applications Enabling' page (**Configuration** tab > **VoIP** menu > **Applications Enabling** submenu > **Applications Enabling**).

Figure 3-67: Applications Enabling Page



2. Save the changes to the device's flash memory and then reset the device (see "Saving Configuration" on page 169).

3.3.2.5 Control Network

The **Control Network** submenu allows you to configure various SIP call control settings. This menu contains the following page items:

- IP Group Table (see Configuring IP Groups on page 103)
- Proxy Sets Table (see Configuring Proxy Sets Table on page 106)

3.3.2.5.1 Configuring IP Groups

The 'IP Group Table' page allows you to create up to nine logical IP entities called *IP Groups*. An IP Group is an entity with a set of definitions such as a Proxy Set ID (see "Configuring Proxy Sets Table" on page 106), which represents the IP address of the IP Group.

IP Groups provide the following uses:

- 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' (see "Configuring Account Table" on page 113).
- Call routing rules:
  - Outgoing IP calls (IP-to-IP or Tel-to-Tel): used to identify the source of the call and used as the destination for the outgoing IP call (defined in the 'Tel to IP Routing'). 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 Hunt Group are sent (defined in "Configuring Hunt Group Settings" on page 126).
  - Incoming IP calls (IP-to-IP or IP-to-Tel): used to identify the source of the IP call
  - Number Manipulation rules to IP: used to associate the rule with a specific calls identified by IP Group.

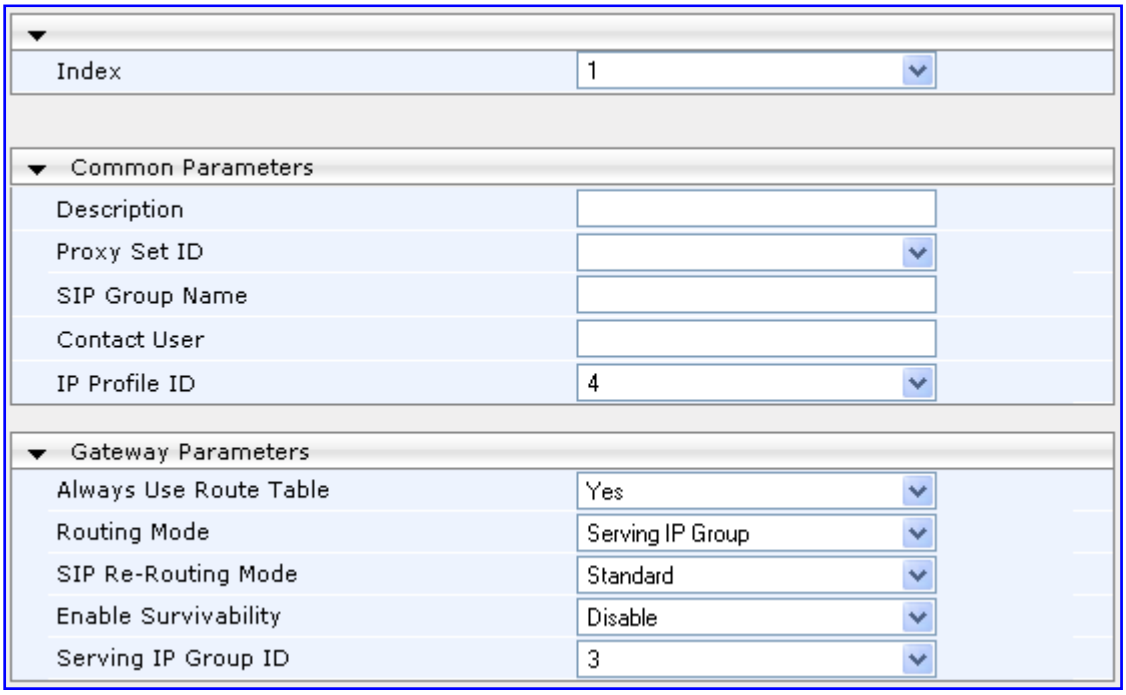
Notes:

- When operating with multiple IP Groups, the default Proxy server must not be used (i.e., the parameter IsProxyUsed must be set to 0).
- You cannot modify IP Group index 0. This IP Group is set to default values and is used by the device when IP Groups are not implemented.
- You can also configure the IP Groups table using the *ini* file table parameter IPGroup (see SIP Configuration Parameters).

➢ **To configure IP Groups:**

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

Figure 3-68: IP Group Table Page



2. Configure the IP group parameters according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" **on page 169.**

Table 3-16: IP Group Parameters

Parameter	Description
Common Parameters	
Description **[IPGroup_Description]**	Brief string description of the IP Group. The value range is a string of up to 29 characters. The default is an empty field.
Proxy Set ID **[IPGroup_ProxySetId]**	The Proxy Set ID (defined in "Configuring Proxy Sets Table" on page 106) associated with the IP Group. All INVITE messages destined to this IP Group are sent to the IP address associated with the Proxy Set. **Note:** Proxy Set ID 0 must **not** be selected; this is the device's default Proxy.
SIP Group Name **[IPGroup_SIPGroupName]**	The SIP Request-URI host name used in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. If not specified, the value of the global parameter, ProxyName (see "Configuring Proxy and Registration Parameters" on page 115) is used instead. The value range is a string of up to 49 characters. The default is an empty field.

Parameter	Description
Contact User **[IPGroup_ContactUser]**	Defines the user part for the From, To, and Contact headers of SIP REGISTER messages, and the user part for the Contact header of INVITE messages that are received from the IP Group and forwarded by the device to another IP Group. **Note:** This parameter is overridden by the 'Contact User' parameter in the 'Account' table (see "Configuring Account Table" on page 113).
IP Profile ID **[IPGroup_ProfileId]**	The IP Profile (defined in to "Configuring IP Profile Settings" on page 122) that you want assigned to this IP Group. The default is 0.
Gateway Parameters	
Always Use Route Table **[IPGroup_AlwaysUseRouteTable]**	Determines the Request-URI host name in outgoing INVITE messages. ▪ **[0]** No (default). ▪ **[1]** Yes = The device uses the IP address (or domain name) defined in the 'Tel to IP Routing' (see "Configuring the Tel to IP Routing" on page 138) as the Request-URI host name in outgoing INVITE messages instead of the value entered in the 'SIP Group Name' field.
SIP Re-Routing Mode **[IPGroup_SIPReRoutingMode]**	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). ▪ **[0]** 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 (default). ▪ **[1]** Proxy = Sends a new INVITE to the Proxy. **Note:** Applicable only if a Proxy server is used and the parameter AlwaysSendtoProxy is set to 0. ▪ **[2]** Routing Table = Uses the Routing table to locate the destination and then sends a new INVITE to this destination. **Notes:** ▪ When this parameter is set to [1] and the INVITE sent to the Proxy fails, the device re-routes the call according to the Standard mode [0]. ▪ When this parameter is set to [2] and the INVITE fails, the device re-routes the call according to the Standard mode [0]. 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. ▪ When this parameter is set to [2], the XferPrefix parameter can be used to define different routing rules for redirected calls. ▪ This parameter is ignored if the parameter AlwaysSendToProxy is set to 1.

3.3.2.5.2 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 10 Proxy Sets, each with a unique ID number and 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 a Proxy Set contains more than one Proxy address).

Proxy Sets can later be assigned to IP Groups of type SERVER (see "Configuring IP Groups" on page 103). 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.

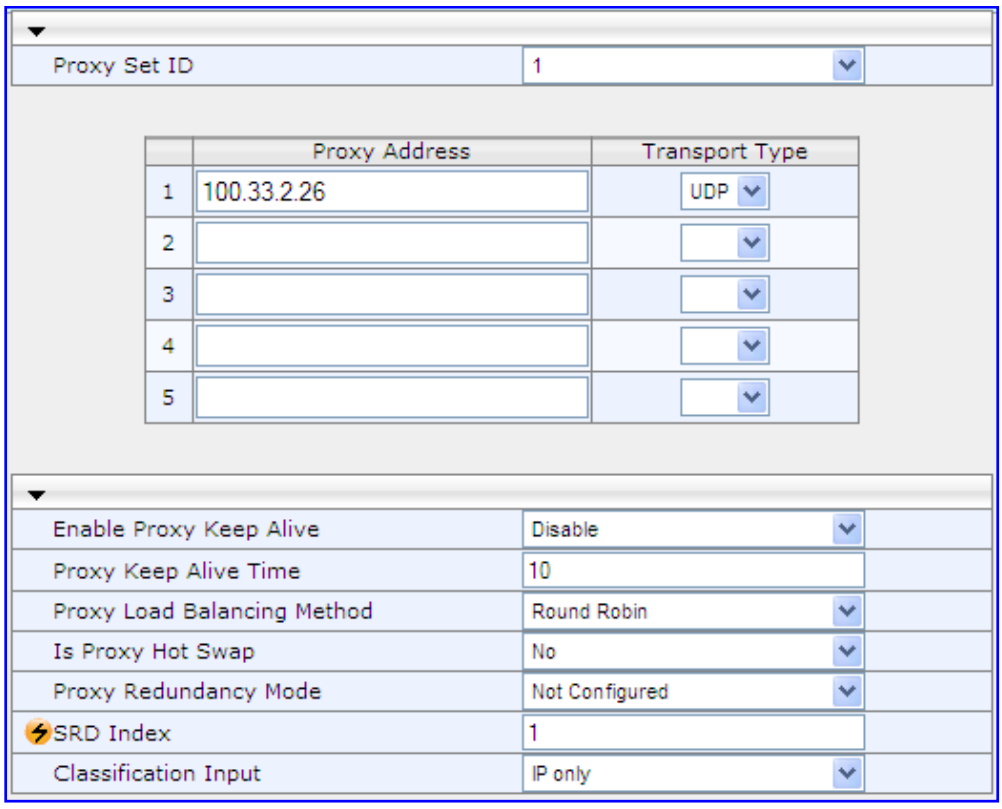
Notes:

- You can also configure the Proxy Sets table using two complementary *ini* file table parameters (see SIP Configuration Parameters):
  - ProxyIP: used for creating a Proxy Set ID defined with IP addresses.
  - ProxySet: used for defining various attributes for the Proxy Set ID.
- Proxy Sets can be assigned only to SERVER-type IP Groups.

➢ **To add Proxy servers:**

1. Open the 'Proxy Sets Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).

Figure 3-69: Proxy Sets Table Page



2. From the 'Proxy Set ID' drop-down list, select an ID for the desired group.
3. Configure the Proxy parameters according to the following table.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.

Table 3-17: Proxy Sets Table Parameters

Parameter	Description
Web: Proxy Set ID EMS: Index **[ProxySet_Index]**	The Proxy Set identification number. The valid range is 0 to 9. The Proxy Set ID 0 is used as the default Proxy Set. **Note:** Although not recommended, you can use both default Proxy Set (ID 0) and IP Groups for call routing. For example, on the 'Hunt Group Settings' page (see "Configuring Hunt Group Settings" on page 126) you can configure a Serving IP Group to where you want to route specific Hunt Group's endpoints, while all other device endpoints use the default Proxy Set. At the same, you can also use IP Groups in the 'Tel to IP Routing' (see "Configuring the Tel to IP Routing" on page 138) to configure the default Proxy Set if the parameter PreferRouteTable is set to 1. To summarize, if the default Proxy Set is used, the INVITE message is sent according to the following preferences: ▪ To the Hunt Group's Serving IP Group ID, as defined in the 'Hunt Group Settings' table. ▪ According to the 'Tel to IP Routing' if the parameter PreferRouteTable is set to 1. ▪ To the default Proxy. 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 113).
Proxy Address **[ProxyIp_IpAddress]**	The IP address (and optionally port number) of the Proxy server. Up to five IP addresses can be configured per Proxy Set. Enter the IP address as an FQDN or in dotted-decimal notation (e.g., 201.10.8.1). You can also specify the selected port in the format: <IP address>:<port>. 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 (*primary*) Proxy defined in the list, the device attempts to communicate with the other (*redundant*) 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. 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). **Notes:** ▪ If EnableProxyKeepAlive is set to 1 or 2, the device monitors the connection with the Proxies by using keep-alive messages (OPTIONS or REGISTER). ▪ To use Proxy Redundancy, you must specify one or more redundant Proxies. ▪ When a port number is specified (e.g., domain.com:5080), DNS NAPTR/SRV queries aren't performed, even if

Parameter	Description
	ProxyDNSQueryType is set to 1 or 2.
Transport Type **[ProxyIp_TransportType]**	The transport type per Proxy server. ▪ **[0]** UDP ▪ **[1]** TCP ▪ **[2]** TLS ▪ **[-1]** = Undefined **Note:** If no transport type is selected, the value of the global parameter SIPTransportType is used (see "Configuring SIP General Parameters" on page 110).
Web/EMS: Enable Proxy Keep Alive **[ProxySet_EnableProxyKeepAlive]**	Determines whether Keep-Alive with the Proxy is enabled or disabled. This parameter is configured per Proxy Set. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Using Options = Enables Keep-Alive with Proxy using SIP OPTIONS messages. ▪ **[2]** Using Register = Enables Keep-Alive with Proxy using SIP REGISTER messages. 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). Any response from the Proxy, either success (200 OK) or failure (4xx response) is considered as if the Proxy is communicating correctly. **Notes:** ▪ This parameter must be set to 'Using Options' when Proxy redundancy is used. ▪ When this parameter is set to 'Using Register', the homing redundancy mode is disabled. ▪ 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. ▪ 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.
Web: Proxy Keep Alive Time EMS: Keep Alive Time **[ProxySet_ProxyKeepAliveTime]**	Defines the Proxy keep-alive time interval (in seconds) between Keep-Alive messages. This parameter is configured per Proxy Set. The valid range is 5 to 2,000,000. The default value is 60. **Note:** 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 parameter RegistrationTime.
Web: Proxy Load Balancing Method EMS: Load Balancing Method **[ProxySet_ProxyLoadBalancingMethod]**	Enables the Proxy Load Balancing mechanism per Proxy Set ID. ▪ **[0]** Disable = Load Balancing is disabled (default) ▪ **[1]** Round Robin ▪ **[2]** Random Weights 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

Parameter	Description
	and ProxyKeepAliveTime) tags each entry as 'offline' or 'online'. Load balancing is only performed on Proxy servers that are tagged as 'online'. All outgoing messages are equally distributed across the list of IP addresses. REGISTER messages are also distributed unless a RegistrarIP is configured. The IP 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. 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: ▪ The Proxy Set includes more than one Proxy IP address. ▪ The only Proxy defined is an IP address and not an FQDN. ▪ SRV is not enabled (DNSQueryType). ▪ The SRV response includes several records with a different Priority value.
Web/EMS: Is Proxy Hot-Swap **[ProxySet_IsProxyHotSwap]**	Enables the Proxy Hot-Swap redundancy mode per Proxy Set. ▪ **[0]** No (default) ▪ **[1]** Yes 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.
Web/EMS: Redundancy Mode **[ProxySet_ProxyRedundancyMode]**	Determines whether the device switches back to the primary Proxy after using a redundant Proxy (per this Proxy Set). ▪ **[-1]** = Not configured – the “global” parameter ProxyRedundancyMode applies (default). ▪ **[0]** Parking = The device continues operating with a redundant (now active) Proxy until the next failure, after which it operates with the next redundant Proxy. ▪ **[1]** Homing = The device always attempts to operate with the primary Proxy server (i.e., switches back to the primary Proxy whenever it's available). **Notes:** ▪ 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. ▪ If this parameter is configured, then the global parameter is ignored.

3.3.2.6 SIP Definitions

The **SIP Definitions** submenu allows you to configure various SIP call control settings. This menu contains the following page items:

- General Parameters (see "Configuring SIP General Parameters" on page 110)
- Advanced Parameters (see "Configuring Advanced Parameters" on page 112)
- Account Table (see "Configuring Account Table" on page 113)
- Proxy & Registration (see "Configuring Proxy and Registration Parameters" on page 115)
- Accounting Settings (see "Configuring Accounting Settings" on page 117)

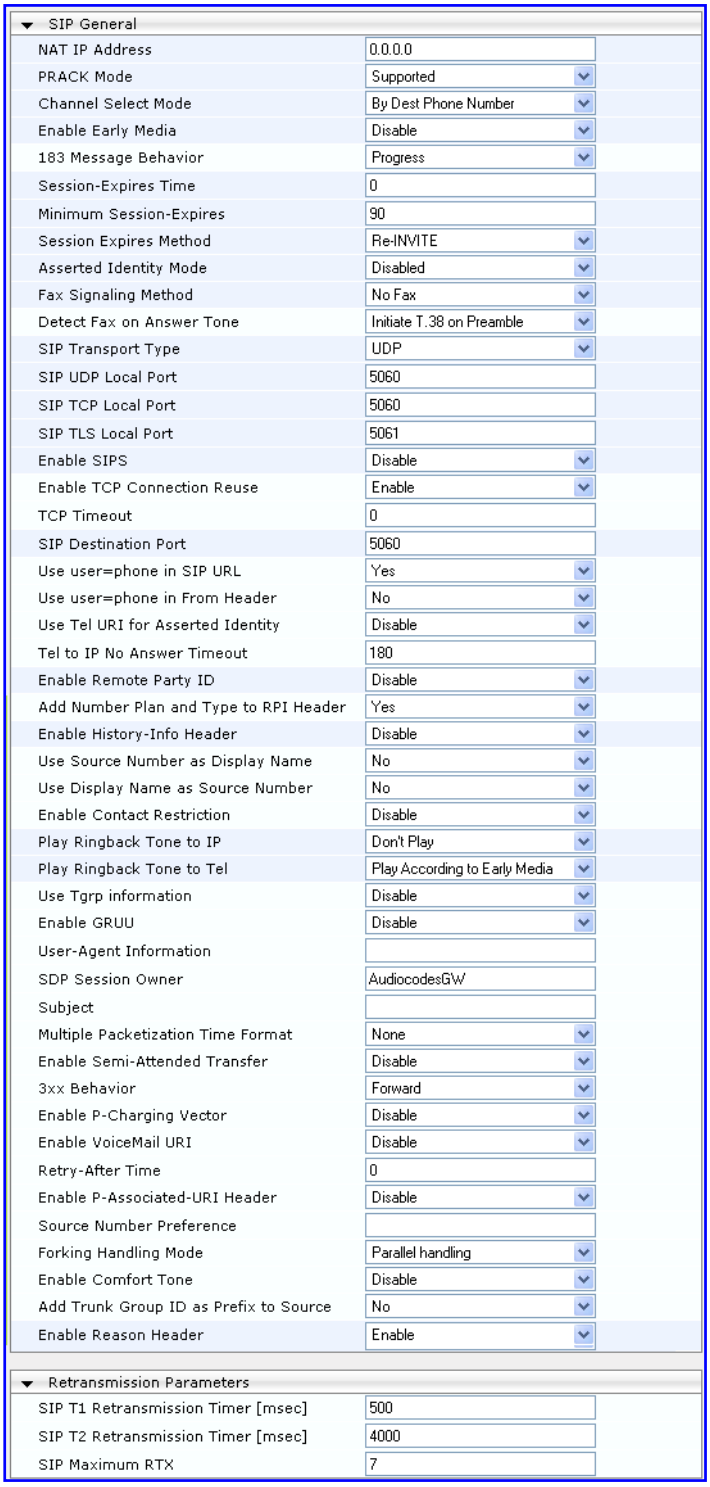
3.3.2.6.1 Configuring SIP General Parameters

The 'SIP General Parameters' page is used to configure general SIP parameters. For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333.

➢ **To configure general SIP parameters:**

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

Figure 3-70: SIP General Parameters Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

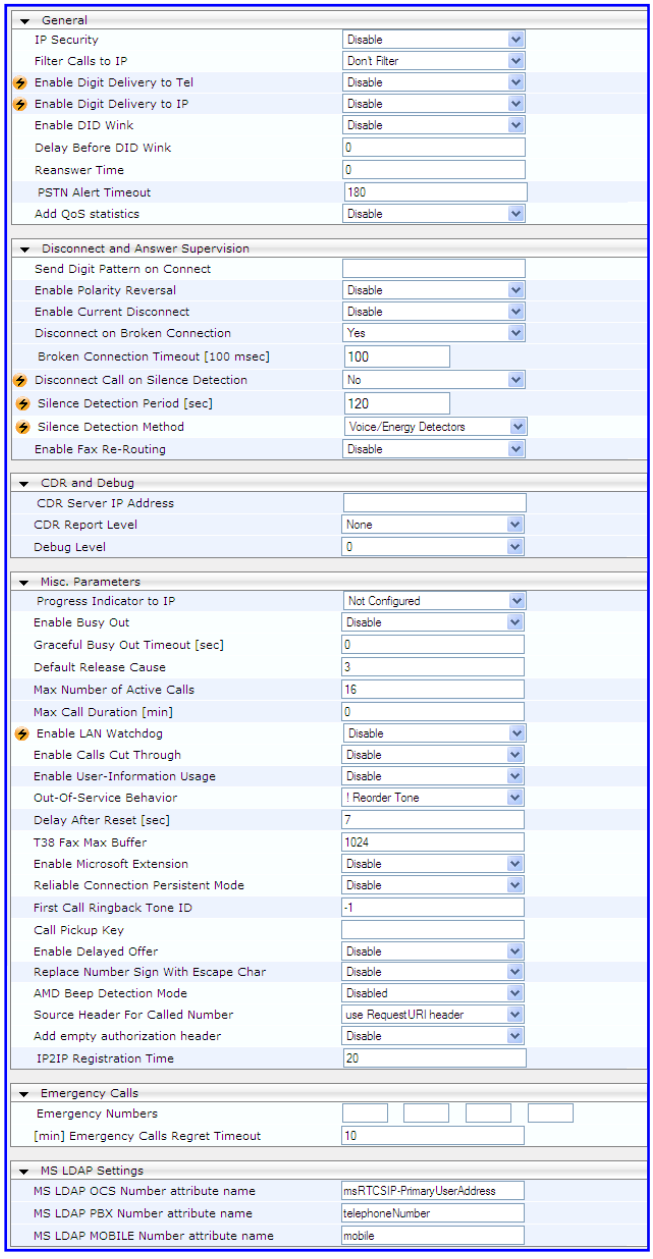
3.3.2.6.2 Configuring Advanced Parameters

The 'Advanced Parameters' page allows you to configure advanced SIP control parameters. For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333.

➢ **To configure advanced general protocol parameters:**

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

Figure 3-71: Advanced Parameters Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.6.3 Configuring Account Table

The 'Account Table' page allows you to define up to 10 *Accounts* per Hunt Group (*Served Hunt Group*) for registration and/or digest authentication (user name and password) to a destination IP address (*Serving IP Group*). The Account table can be used, for example, to register to an Internet Telephony Service Provider (ITSP) on behalf of an IP-PBX to which the device is connected. The registrations are sent to the Proxy Set ID (see "Configuring Proxy Sets Table" on page 106) associated with these Serving IP Groups.

A Hunt Group can register to more than one Serving IP Group (e.g., ITSP's). This can be achieved by configuring multiple entries in the Account table with the same Served Hunt 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 (to a Proxy server), if all trunks pertaining 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.

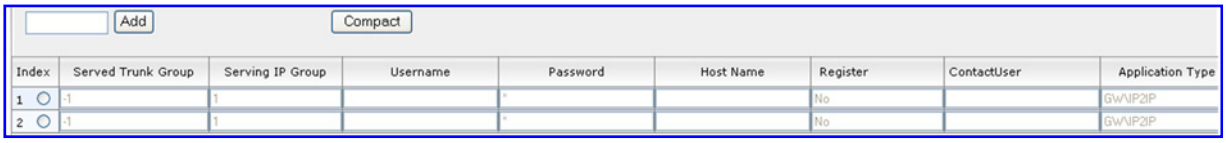
Notes:

- For viewing Account registration status, see "Viewing Registration Status" on page 189.
- You can also configure the Account table using the *ini* file table parameter Account (see SIP Configuration Parameters).

➢ **To configure Accounts:**

1. Open the 'Account Table' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Account Table**).

Figure 3-72: Account Table Page



2. To add an Account, 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 169.

Note: For a description of the Web interface's table command buttons (e.g., **Duplicate** and **Delete**), see "Working with Tables" on page 39.

Table 3-18: Account Table Parameters Description

Parameter	Description
Served Trunk Group **[Account_ServedTrunkGroup]**	The Hunt Group ID for which you want to register and/or authenticate to a destination IP Group (i.e., Serving IP Group). For Tel-to-IP calls, the Served Hunt Group is the source Hunt Group from where the call originated. For IP-to-Tel calls, the Served Hunt Group is the 'Hunt Group ID' defined in the 'IP to Hunt Group Routing Table' (see "Configuring the IP to Hunt Group Routing Table" on page 142). For defining Hunt Groups, seeto Configuring Endpoint Phone Numbers on page 124.
Serving IP Group **[Account_ServingIPGroup]**	The destination IP Group ID (defined in "Configuring IP Groups" on page 103) to where the REGISTER requests (if enabled) are sent or authentication is performed. The actual destination to where the REGISTER requests are sent is the IP address defined for the Proxy Set ID (see "Configuring Proxy Sets Table" on page 106) associated with the IP Group. This occurs only in the following conditions: ▪ The parameter 'Registration Mode' is set to 'Per Account' in the 'Hunt Group Settings' table (see "Configuring Hunt Group Settings" on page 126). ▪ The parameter 'Register' in this table is set to 1. In addition, for a SIP call that is identified by both the Served Hunt Group and Serving IP Group, the username and password for digest authentication defined in this table is used. For Tel-to-IP calls, the Serving IP Group is the destination IP Group defined in the 'Hunt Group Settings' table or 'Tel to IP Routing' (see "Configuring the Tel to IP Routing" on page 138). For IP-to-Tel calls, the Serving IP Group is the 'Source IP Group ID' defined in the 'IP to Hunt Group Routing Table' (see "Configuring the IP to Hunt Group Routing Table" on page 142). **Note:** If no match is found in this table for incoming or outgoing calls, the username and password defined in the 'Authentication' table (see "Configuring Authentication" on page 153) or the global parameters (UserName and Password) defined on the 'Proxy & Registration' page.
Username **[Account_Username]**	Digest MD5 Authentication user name (up to 50 characters).
Password **[Account_Password]**	Digest MD5 Authentication password (up to 50 characters). **Note:** After you click the **Apply** button, this password is displayed as an asterisk (*).
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 HostName is also included in the INVITE request's From header URI. If not configured or if registration fails, the 'SIP Group Name' parameter from the 'IP Group' table is used instead. This parameter can be up to 49 characters.

Parameter	Description

Register
[Account_Register]
	Enables registration.
	▪ **[0]** No = Don't register
	▪ **[1]** Yes = Enables registration
	When enabled, the device sends REGISTER requests to the Serving IP Group. In addition, to activate registration, you also need to set the parameter 'Registration Mode' to 'Per Account' in the 'Hunt Group Settings' table for the specific Hunt 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 a successful registration. See the example below:
	`REGISTER sip:xyz SIP/2.0`
	`Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac1397582418`
	`From: <sip:ContactUser@HostName>;tag=1c1397576231`
	`To: <sip: ContactUser@HostName >`
	`Call-ID: 13975689572612000222256@10.33.37.78`
	`CSeq: 1 REGISTER`
	`Contact: <sip:ContactUser@10.33.37.78>;expires=3600`
	`Expires: 3600`
	`User-Agent: Sip-Gateway/v.6.00A.008.002`
	`Content-Length: 0`
	Notes:
	▪ The Hunt Group account registration is not affected by the parameter IsRegisterNeeded.
	▪ If registration to an IP Group(s) fails for **all** the accounts defined in this table for a specific Hunt Group, and if this Hunt Group includes all the channels in the Hunt Group, the Hunt Group is set to Out-Of-Service if the parameter OOSOnRegistrationFail is set to 1 (see "Proxy & Registration Parameters" on page 115).

Contact User **[Account_ContactUser]**	Defines the AOR user name. It appears in REGISTER From/To headers as ContactUser@HostName, and in INVITE/200 OK Contact headers as ContactUser@<device's IP address>. If not configured, the 'Contact User' parameter from the 'IP Group Table' page is used instead. **Note:** If registration fails, then the user part in the INVITE Contact header contains the source party number.
Application Type **[Account_ApplicationType]**	**Note:** This parameter is not applicable.

3.3.2.6.4 Configuring Proxy and Registration Parameters

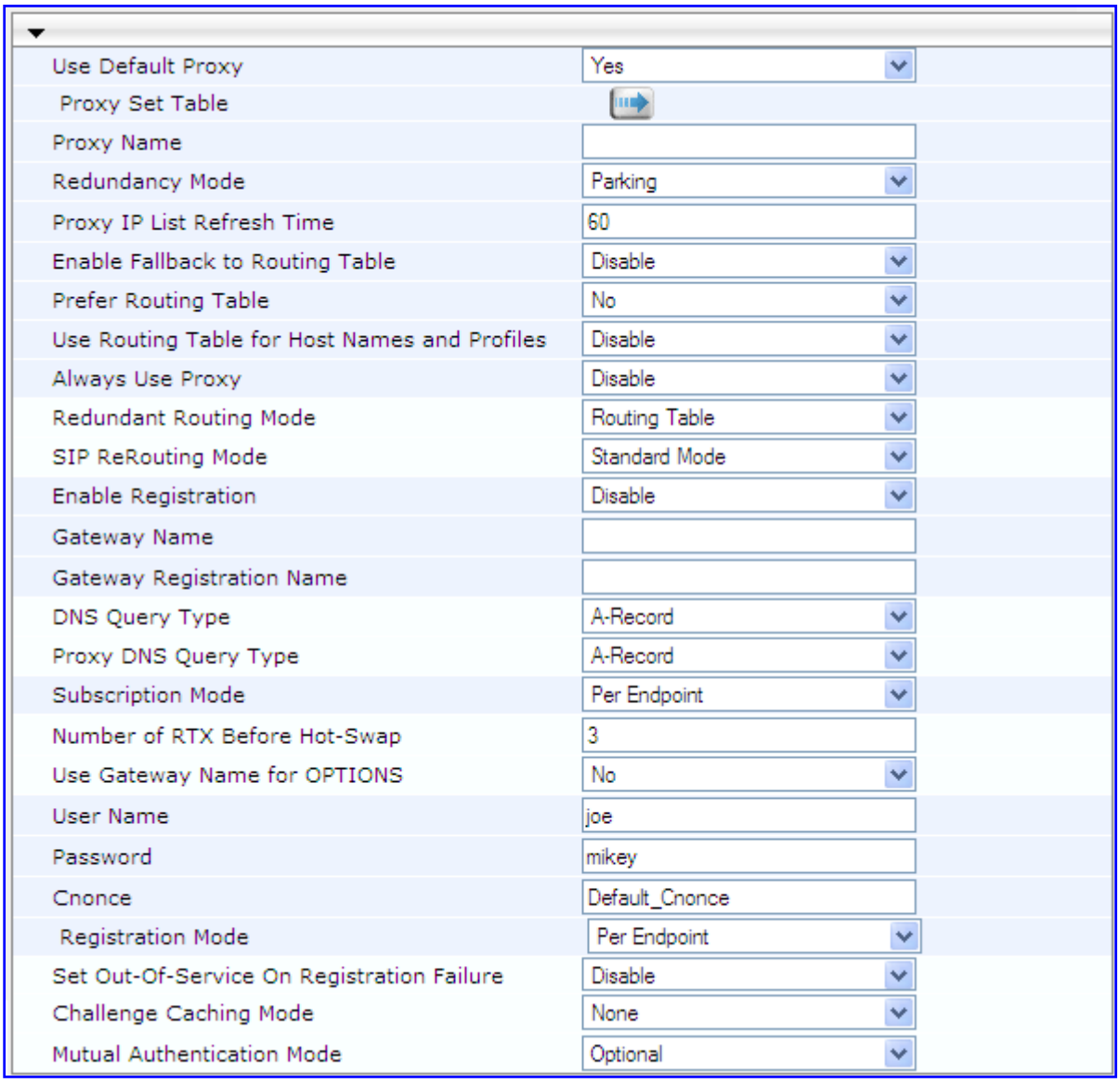
The 'Proxy & Registration' page allows you to configure the Proxy server and registration parameters. For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333.

Note: To view whether the device or its endpoints have registered to a SIP Registrar/Proxy server, see "Viewing Registration Status" on page 189.

➢ **To configure the Proxy and registration parameters:**

1. Open the 'Proxy & Registration' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Proxy & Registration**).

Figure 3-73: Proxy & Registration Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. Click the **Register** or **Un-Register** buttons to save your changes and register/unregister to a Proxy/Registrar.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.

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 106 for a description of this page).

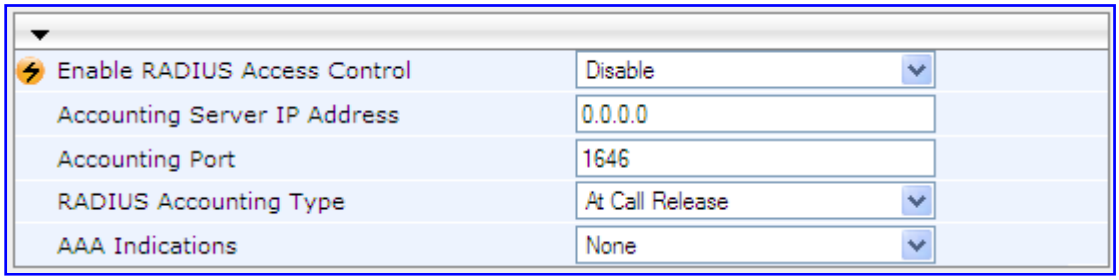
3.3.2.6.5 Configuring Accounting Settings

The 'RADIUS Parameters' page allows you to configure the RADIUS parameters. For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333.

➢ **To configure the RADIUS parameters:**

1. Open the 'RADIUS Parameters' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Accounting Settings**).

Figure 3-74: RADIUS Parameters Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.7 Coders and Profiles

The **Coders And Profile Definitions** submenu includes the following page items:

- Coders (see "Configuring Coders" on page 118)
- Coders Group Settings (see "Configuring Coder Groups" on page 119)
- Tel Profile Settings (see "Configuring Tel Profiles" on page 121)
- IP Profile Settings (see "Configuring IP Profiles" on page 122)

Implementing the device's Profile features provides the device with high-level adaptation when connected to a variety of equipment (at both Tel and IP sides) and protocols, each of which requires different system behavior. Each Profile contains a set of parameters such as coders, T.38 Relay, Voice and DTMF Gain, Silence Suppression, Echo Canceler, RTP DiffServ, Current Disconnect and more. The Profiles feature allows you to customize these parameters or turn them on or off, per source or destination routing and/or per the device's endpoints (channels). For example, specific ports can be assigned a Profile that always uses G.711.

Each call can be associated with one or two Profiles - Tel Profile and/or IP Profile. If both IP and Tel Profiles apply to the same call, the coders and other common parameters of the preferred Profile (determined by the Preference option) are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters take precedence.

You can assign different Profiles (behavior) per call, using the call routing tables:

- 'Tel to IP Routing' page (see Configuring the Tel to IP Routing on page 138)
- 'IP to Hunt Group Routing Table' page (see Configuring the IP to Hunt Group Routing Table on page 142)

In addition, you can associate different Profiles per the channels.

Notes:

- The default values of the parameters in the 'Tel Profile Settings' and 'IP Profile Settings' pages are identical to their default values in their respective primary configuration page ("global" parameter).
- If you modify a global parameter in its primary configuration page (or ini file) that also appears in a profile pages, the parameter's new value is automatically updated in the profile page. However, once you modify any parameter in a profile page, modifications to parameters in the primary configuration pages (or ini file) no longer impact that profile page.

3.3.2.7.1 Configuring Coders

The 'Coders' page allows you to configure up to 10 coders for the device. The first coder in the list has the highest priority and is used by the device whenever possible. If the far-end device cannot use the first coder, the device attempts to use the next coder in the list, and so on.

Notes:

- For a list of supported coders and for configuring coders using the *ini* file, refer to the *ini* file parameter table CodersGroup, described in SIP Configuration Parameters.
- For defining groups of coders (which can be assigned to Tel and IP Profiles), see "Configuring Coder Groups" on page 119.
- For an explanation on V.152 support (and implementation of T.38 and VBD coders), see "Supporting V.152 Implementation" on page 253.

➢ **To configure the device's coders:**

1. Open the 'Coders' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **Coders**).

Figure 3-75: Coders 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 the **Submit** button to save your changes.
9. To save the changes to flash memory, see "Saving Configuration" on page 169.

Notes:

- A coder (i.e., 'Coder Name') can appear only 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.
- For G.729, it's also possible to select silence suppression without adaptations.
- If the coder G.729 is selected with 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).

3.3.2.7.2 Configuring Coder Groups

The 'Coder Group Settings' page allows you to define up to four different Coder Groups. These Coder Groups can be assigned to Tel Profiles (see Configuring Tel Profiles on page 121) and/or IP Profiles (see Configuring IP Profiles on page 122). For each Coder Group, you can define up to ten coders, where the first coder in the table takes precedence over the second coder, and so on. The first coder is the highest priority coder and is used by the device whenever possible. If the far end device cannot use the first coder, the device attempts to use the next coder, and so on.

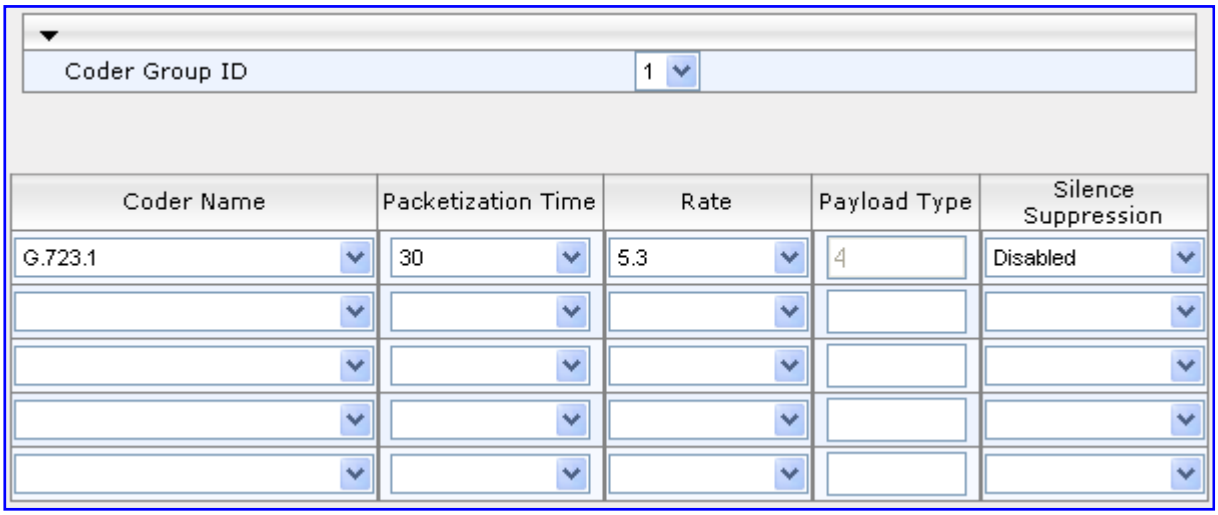
Notes:

- A coder type can appear only once per Coder Group.
- For a list of supported coders and for configuring coders using the *ini* file, refer to the *ini* file parameter table CodersGroup, described in SIP Configuration Parameters.
- For information on coders, refer to the notes in "Configuring Coders" on page 118.

➢ **To configure Coder Groups:**

1. Open the 'Coder Group Settings' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **Coders Group Settings**).

Figure 3-76: Coder Group Settings Page



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 'well-known' 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 the **Submit** button to save your changes.
11. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.7.3 Configuring Tel Profile

The 'Tel Profile Settings' page allows you to define up to nine Tel Profiles. You can assign these Tel Profiles to the device's channels in the <Endpoint Phone Number Table (see Configuring Endpoint Phone Numbers on page 124), and thereby, apply different behaviors to different channels.

Note: You can also configure Tel Profiles using the *ini* file table parameter TelProfile (see SIP Configuration Parameters).

➢ **To configure Tel Profiles:**

1. Open the 'Tel Profile Settings' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **Tel Profile Settings**).

Figure 3-77: Tel Profile Settings Page

2. From the 'Profile ID' drop-down list, select the Tel Profile identification number you want to configure.
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' is 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 Profile's parameters according to your requirements. For detailed information on each parameter, refer to the description of the "global" parameter.
6. From the 'Coder Group' drop-down list, select the Coder Group (see "Configuring Coder Groups" on page 119) or the device's default coder (see "Configuring Coders" on page 118) to which you want to assign the Profile.
7. Repeat steps 2 through 6 to configure additional Tel Profiles (optional).
8. Click the **Submit** button to save your changes.
9. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.7.4 Configuring IP Profiles

The 'IP Profile Settings' page allows you to define up to nine IP Profiles. You can later assign these IP Profiles to other configuration entities:

- Tel to IP Routing (see "Configuring Tel to IP Routing" on page 138)
- IP to Hunt Group Routing Table (see "Configuring IP to Hunt Group Routing Table" on page 142)
- IP Group (see "Configuring IP Groups" on page 103)

The 'IP Profile Settings' page conveniently groups parameters according to application to which they pertain:

- Common Parameters: parameters common to all application types
- Gateway Parameters: parameters applicable to gateway functionality

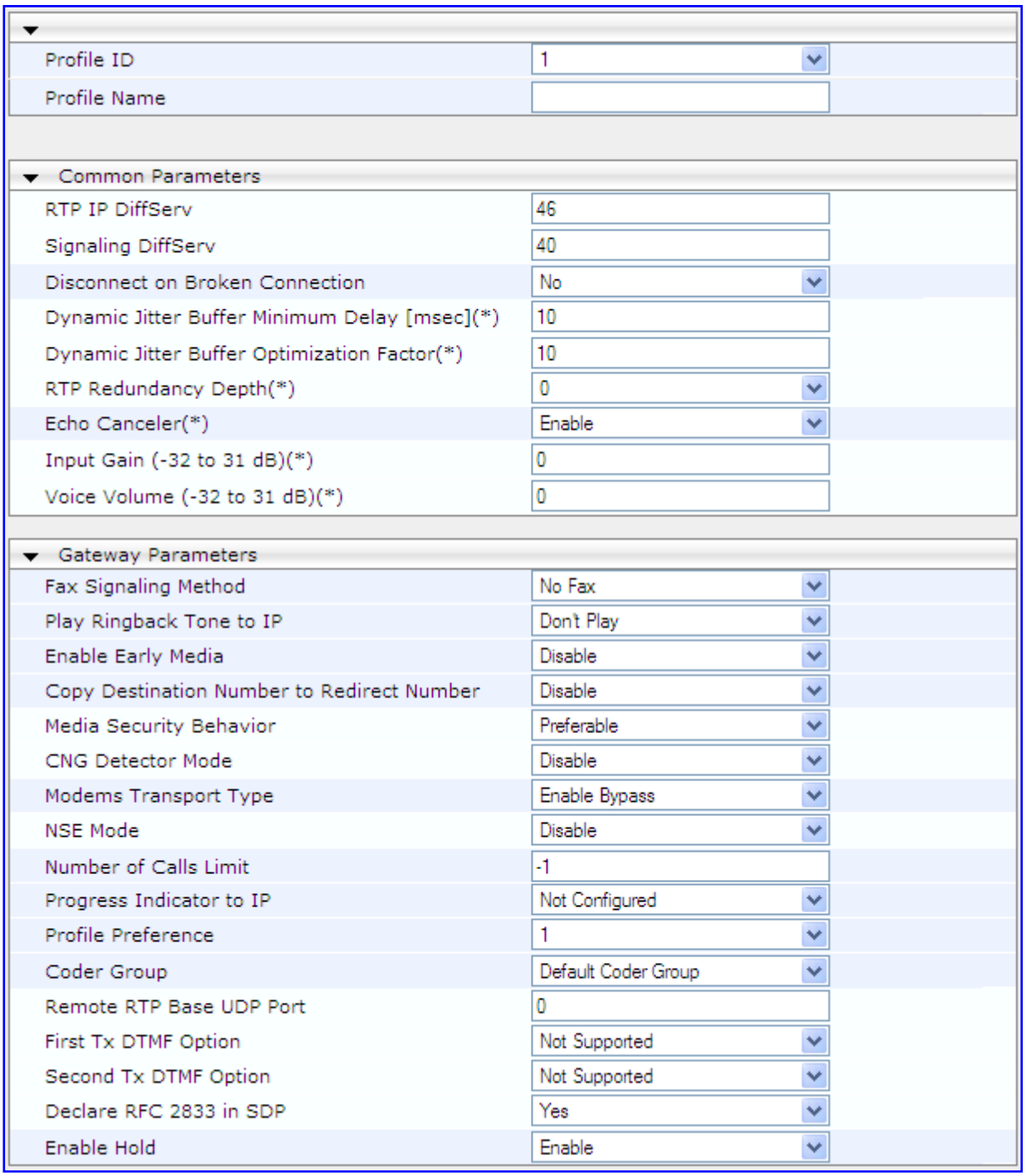
Notes:

- For a detailed description of each parameter, refer to its corresponding "global" parameter (configured as an individual parameter).
- IP Profiles can also be implemented when operating with a Proxy server (when the parameter AlwaysUseRouteTable is set to 1).
- You can also configure IP Profiles using the *ini* file table parameter IPProfile (see SIP Configuration Parameters).

➢ **To configure IP Profiles:**

1. Open the 'IP Profile Settings' page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **IP Profile Settings**).

Figure 3-78: IP Profile Settings Page



2. From the 'Profile ID' drop-down list, select an identification number for the IP Profile.
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 IP Profile's parameters according to your requirements.
6. From the 'Coder Group' drop-down list, select the coder group that you want to assign to the IP Profile. You can select the device's default coders (see "Configuring Coders" on page 118), or one of the coder groups you defined in the 'Coder Group Settings' page (see "Configuring Coder Groups" on page 119).
7. Repeat steps 2 through 6 for the next IP Profiles (optional).
8. Click the **Submit** button to save your changes.
9. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.8 GW and IP to IP

The **GW and IP to IP submenu** configures the gateway as well as IP-to-IP parameters and includes the following page items:

- Trunk Group (see "Hunt Group" on page 124)
- Manipulations (see "Manipulation" on page 129)
- Routing (see "Routing" on page 137)
- DTMF and Supplementary (see "DTMF and Supplementary" on page 147)
- Analog Gateway (see "Analog Gateway" on page 149)
- Advanced Applications (see "Advanced Applications" on page 160)

3.3.2.8.1 Hunt Group

The **Hunt Group** submenu allows you to configure groups of channels called Hunt Groups. This submenu includes the following page items:

- Endpoint Phone Number (see "Configuring Endpoint Phone Numbers" on page 124)
- Hunt Group Settings (see "Configuring Hunt Group Settings" on page 126)

3.3.2.8.1.1 Configuring Endpoint Phone Numbers

The 'Endpoint Phone Number Table' page allows you to activate the device's ports (channels or endpoints), by defining telephone numbers for the endpoints and assigning them to Hunt Groups and Tel Profiles.

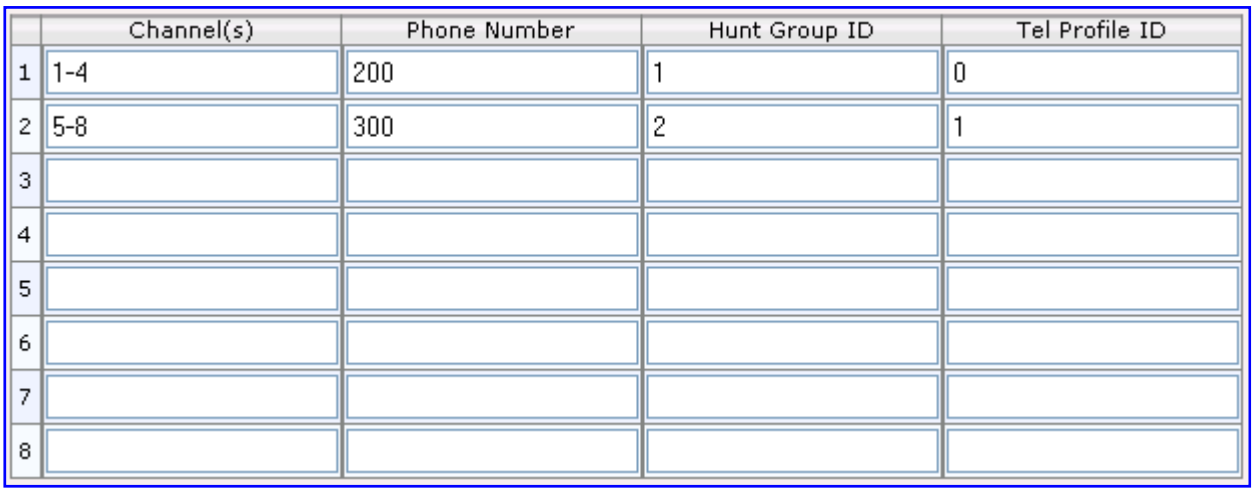
Notes:

- Each endpoint must be assigned a unique phone number. In other words, no two endpoints can have the same phone number.
- The number of endpoints depends on the MediaPack model (e.g., MP-118 displays 8 endpoints).
- You can also configure the endpoint phone numbers using the *ini* file table parameter TrunkGroup (see "Number Manipulation and Routing Parameters" on page 474).

➢ **To configure the Endpoint Phone Number table:**

1. Open the 'Endpoint Phone Number Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP submenu** > **Hunt Group** submenu > **Endpoint Phone Number**).

Figure 3-79: Endpoint Phone Number Table Page



	Channel(s)	Phone Number	Hunt Group ID	Tel Profile ID
1	1-4	200	1	0
2	5-8	300	2	1
3				
4				
5				
6				
7				
8				

2. Configure the endpoint phone numbers according to the table below. You must enter a number in the 'Phone Number' fields for each port that you want to use.
3. Click the **Submit** button to save your changes, or click the **Register** or **Un-Register** buttons to save your changes and to register/unregister to a Proxy/Registrar.
4. To save the changes to the flash memory, see "Saving Configuration" on page 169.

Table 3-19: Endpoint Phone Number Table Parameters

Parameter	Description
Channel(s)	The device's channels or ports as labeled on the device's rear-panel. To enable channels, enter the channel (port) numbers. You can enter a range of channels by using the format [n-m], where *n* represents the lower channel number and *m* the higher channel number, e.g., [1-3] specifies channels (ports) 1 through 3.
Phone Number	The telephone number that is assigned to the channel. This value can include 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 phone numbers are also used for channel allocation for IP-to-Tel calls if the Hunt Group's Channel Select Mode is set to 'By Dest Phone Number'. **Note:** 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').

Parameter	Description
Hunt Group ID	The Hunt Group ID (1-99) assigned to the corresponding channels. The same Hunt Group ID can be assigned to more than one group of channels. The Hunt Group ID is used to define a group of common channel behaviors that are used for routing IP-to-Tel calls. If an IP-to-Tel call is assigned to a Hunt Group, the call is routed to the channel(s) pertaining to that Hunt Group ID. **Notes:** ▪ Once you have defined a Hunt Group, you must configure the parameter PSTNPrefix ('IP to Hunt Group Routing Table') to assign incoming IP calls to the appropriate Hunt Group. If you do not configure this table, calls cannot be established. ▪ You can define the method for which calls are assigned to channels within the Hunt Groups, using the parameter TrunkGroupSettings.
Tel Profile ID	The Tel Profile ID assigned to the channels. **Note:** For configuring Tel Profiles, see the parameter TelProfile.

3.3.2.8.1.2 Configuring Hunt Group Settings

The 'Hunt Group Settings' page allows you to configure the settings of up to 24 Hunt Groups. These Hunt Groups are configured in the 'Endpoint Phone Number Table' page (see Configuring Endpoint Phone Numbers on page 124).

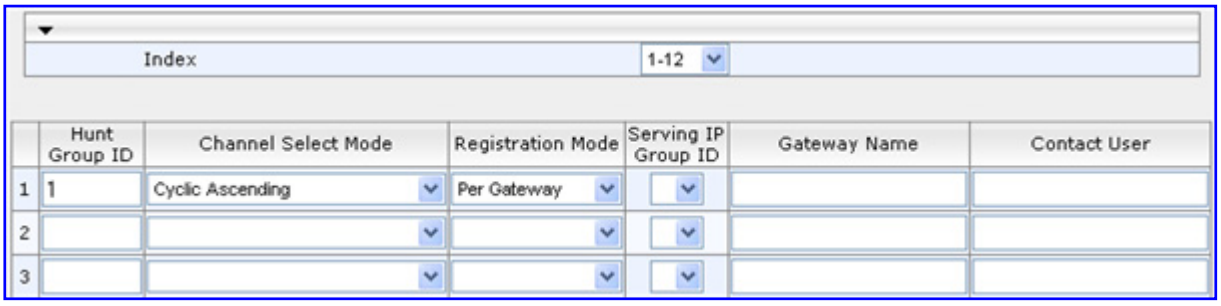
This page allows you to select the method for which IP-to-Tel calls are assigned to channels within each Hunt Group. If no method is selected for a specific Hunt Group, the setting of the global parameter, ChannelSelectMode takes effect. In addition, this page defines the method for registering Hunt Groups to selected Serving IP Group IDs (if defined).

Note: You can also configure the 'Hunt Group Settings' table using the *ini* file table parameter TrunkGroupSettings (see "Number Manipulation and Routing Parameters" on page 474).

➢ **To configure the Hunt Group Settings table:**

1. Open the 'Hunt Group Settings' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP submenu** > **Hunt Group** submenu > **Hunt Group Settings**).

Figure 3-80: Hunt Group Settings Page



2. From the 'Index' drop-down list, select the range of entries that you want to edit.
3. Configure the Hunt Group according to the table below.
4. Click the **Submit** button to save your changes.

5. To save the changes to flash memory, see "Saving Configuration" on page 169.

An example is shown below of a REGISTER message for registering endpoint "101" using registration Per Endpoint mode. The "SipGroupName" in the Request-URI is defined in the IP Group table (see "Configuring IP Groups" on page 103).

```
REGISTER sip:SipGroupName SIP/2.0
Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac862428454
From: <sip:101@GatewayName>;tag=1c862422082
To: <sip:101@GatewayName>
Call-ID: 990797706251200023282 5@10.33.37.78
CSeq: 3 REGISTER
Contact: <sip:101@10.33.37.78>;expires=3600
Expires: 3600
User-Agent: Sip-Gateway-MP-118 FXS_FXO/v.6.00A.008.002
Content-Length: 0
```

Table 3-20: Hunt Group Settings Parameters

Parameter	Description
Hunt Group ID **[TrunkGroupSettings_TrunkGroupId]**	The Hunt Group ID that you want to configure.
Channel Select Mode **[TrunkGroupSettings_ChannelSelectMode]**	The method for which IP-to-Tel calls are assigned to channels pertaining to a Hunt Group. For a detailed description of this parameter, refer to the global parameter ChannelSelectMode. ▪ **[0]** By Dest Phone Number. ▪ **[1]** Cyclic Ascending (default) ▪ **[2]** Ascending ▪ **[3]** Cyclic Descending ▪ **[4]** Descending ▪ **[5]** Dest Number + Cyclic Ascending ▪ **[6]** By Source Phone Number ▪ **[9]** Ring to Hunt Group (applicable only to FXS interfaces) ▪ **[10]** Select Trunk by Supplementary Services Table (applicable only to BRI interfaces) **Note:** For a detailed description of these options, refer to the "global" ChannelSelectMode parameter.
Registration Mode **[TrunkGroupSettings_RegistrationMode]**	Registration method for the Hunt Group: ▪ **[1]** Per Gateway = Single registration for the entire device (default). This mode is applicable only if a default Proxy or Registrar IP are 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. ▪ **[0]** Per Endpoint = Each channel in the Hunt Group registers individually. The registrations are sent to the ServingIPGroupID if defined in the table, otherwise to the default Proxy, and if no default Proxy, then to the Registrar IP. ▪ **[4]** Don't Register = No registrations are sent by endpoints pertaining to the Hunt Group. For example, if the device is

Parameter	Description
	configured globally to register all its endpoints (using the parameter ChannelSelectMode), you can exclude some endpoints from being registered by assigning them to a Hunt Group and configuring the Hunt Group registration mode to 'Don't Register'. ▪ **[5]** 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 113). **Notes:** ▪ To enable Hunt Group registrations, configure the global parameter IsRegisterNeeded to 1. This is unnecessary for 'Per Account' registration mode. ▪ If no mode is selected, the registration is performed according to the global registration parameter ChannelSelectMode. ▪ If the device is configured globally (ChannelSelectMode) to register Per Endpoint, and endpoints group comprising four FXO endpoints is configured to register Per Gateway, the device registers all endpoints except the first four endpoints. The endpoints Group of these four endpoints sends a single registration request.
Serving IP Group ID **[TrunkGroupSettings_ServingIPGroup]**	The Serving IP Group ID to where INVITE messages initiated by this Hunt Group's endpoints are sent. The actual destination to where these INVITE messages are sent is according to the Proxy Set ID (see "Configuring Proxy Sets Table" on page 106) associated with this Serving 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 field 'SIP Group Name' defined in the 'IP Group' table (see "Configuring IP Groups" on page 103). If no Serving IP Group ID is selected, the INVITE messages are sent to the default Proxy or according to the 'Tel to IP Routing' (see "Configuring Tel to IP Routing" on page 138). **Note:** If the parameter PreferRouteTable is set to 1 (see "Configuring Proxy and Registration Parameters" on page 115), the routing rules in the 'Outbound IP Routing Table'prevail over the selected Serving IP Group ID.
Gateway Name **[TrunkGroupSettings_GatewayName]**	The host name used in the SIP From header in INVITE messages, and as a host name in From/To headers in REGISTER requests. If not configured, the global parameter SIPGatewayName is used instead.
Contact User **[TrunkGroupSettings_ContactUser]**	The user part in the SIP Contact URI in INVITE messages, and as a user part in From, To, and Contact headers in REGISTER requests. This is applicable only if the field 'Registration Mode' is set to 'Per Account', and the Registration through the Account table is successful. **Notes:** ▪ If registration fails, then the user part in the INVITE Contact header contains the source party number. ▪ The 'Contact User' parameter in the 'Account Table' page overrides this parameter.

3.3.2.8.2 Manipulation

The **Manipulation Tables** submenu allows you to configure number manipulation and mapping of NPI/TON to SIP messages. This submenu includes the following items:

- General Settings (see "Configuring General Settings" on page 129)
- Manipulation tables (see "Configuring Number Manipulation Tables" on page 129):
  - Dest Number IP->Tel
  - Dest Number Tel->IP
  - Source Number IP->Tel
  - Source Number Tel->IP
- Redirect Number Tel->IP (see "Configuring Redirect Number Tel to IP" on page 133)
- Phone Context (see "Mapping NPI/TON to SIP Phone-Context" on page 135)

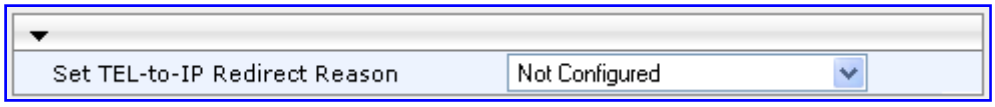
3.3.2.8.2.1 Configuring General Settings

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 333.

➢ **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 3-81: General Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.8.2.2 Configuring Number Manipulation Tables

The device provides number manipulation tables for incoming (IP-to-Tel) and outgoing (Tel-to-IP) calls. These tables are used to modify the destination and/or source telephone numbers so that the calls can be routed correctly. For example, telephone number manipulation can be implemented by 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 detailed information on Caller ID, see Configuring Caller Display Information on page 155.

Number manipulation is configured in the following tables:

- **Tel-to-IP calls:**
  - Destination Phone Number Manipulation Table for Tel-to-IP Calls (NumberMapTel2IP *ini* file parameter) - up to 120 entries
  - Source Phone Number Manipulation Table for Tel-to-IP Calls (SourceNumberMapTel2IP *ini* file parameter) - up to 20 entries

- **IP-to-Tel calls:**
  - Destination Phone Number Manipulation Table for IP-to-Tel Calls (NumberMapIP2Tel *ini* file parameter) - up to 100 entries
  - Source Phone Number Manipulation Table for IP-to-Tel Calls (SourceNumberMapIP2Tel *ini* file parameter) - up to 20 entries

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:

- PerformAdditionalIP2TELSourceManipulation for source number manipulation
- PerformAdditionalIP2TELDestinationManipulation for destination number manipulation

Notes:

- Number manipulation can occur before or after a routing decision is made. For example, you can route a call to a specific Hunt 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 (RouteModeIP2Tel) described in "Configuring IP to Hunt Group Routing Table" on page 142, and 'Tel to IP Routing Mode' parameter (RouteModeTel2IP) described in "Configuring Tel to IP Routing" on page 138.
- Manipulation rules are done in the following order: 1) Stripped digits from left, 2) Stripped digits from right, 3) Number of digits to leave, 4) Prefix to add, and then 5) Suffix to add.
- The manipulation rules can be applied to any incoming call whose source IP address, source Hunt Group, source IP Group, destination number prefix, and/or source number prefix match the values defined in the 'Source IP Address', 'Source Trunk Group', 'Source IP Group', 'Destination Prefix', and 'Source Prefix' fields respectively. The number manipulation can be performed using a combination of each of the above criteria or using each criterion independently.
- For available notations representing multiple numbers/digits for destination and source prefixes, see "Dialing Plan Notation for Routing and Manipulation" on page 228.
- For configuring number manipulation using *ini* file table parameters NumberMapIP2Tel, NumberMapTel2IP, SourceNumberMapIP2Tel, and SourceNumberMapTel2IP, see "Number Manipulation and Routing Parameters" on page 474.

➢ **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 (e.g., 'Source Phone Number Manipulation Table for Tel→IP Calls' page).

Figure 3-82: Source Phone Number Manipulation Table for Tel-to-IP Calls

Index	Source Trunk Group	Source IP Group	Destination Prefix	Source Prefix	Stripped Digits From Left
1	-1	2	03	201	0
2	0	0		1001	4
3	-1	-1	*	123451001#	0
4	-1	-1	*	[30-40]x	0
5	-1	-1	[6,7,8]	2001	5

Stripped Digits From Right	Prefix to Add	Suffix to Add	Number of Digits to Leave	Presentation
0	971		255	Allowed
0	5	23	255	Restricted
0		8	4	Not Configured
1	2		255	Not Configured
0	3		255	Not Configured

The figure above shows an example of the use of manipulation rules for Tel-to-IP source phone number manipulation:

- **Index 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.
- **Index 2:** When the source number has prefix 1001 (e.g., 1001876), it is changed to 587623.
- **Index 3:** When the source number has prefix 123451001 (e.g., 1234510012001), it is changed to 20018.
- **Index 4:** When the source number has prefix from 30 to 40 and a digit (e.g., 3122), it is changed to 2312.
- **Index 5:** When the destination number has the prefix 6, 7, or 8 (e.g., 85262146), source number prefix 2001, it is changed to 3146.

2. Configure the Number Manipulation table according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

Table 3-21: Number Manipulation Parameters Description

Parameter	Description
Source Trunk Group	The source Hunt Group ID for Tel-to-IP calls. To denote all Hunt Groups, leave this field empty. **Notes:** ▪ The value -1 indicates that this field is ignored in the rule. ▪ This parameter is available only in the 'Source Phone Number Manipulation Table for Tel -> IP Calls' and 'Destination Phone Number Manipulation Table for Tel -> IP Calls' pages. ▪ For IP-to-IP call routing, this parameter is not required (i.e., leave the field empty).
Source IP Group	The IP Group from where the IP-to-IP call originated. Typically, this IP Group of an incoming INVITE is determined/classified using the 'IP to Hunt Group Routing Table'. If not used (i.e., any IP Group), simply leave the field empty. **Notes:** ▪ The value -1 indicates that this field is ignored in the rule. ▪ This parameter is available only in the 'Source Phone Number Manipulation Table for Tel -> IP Calls' and 'Destination Phone Number Manipulation Table for Tel -> IP Calls' pages. ▪ If this Source IP Group has a Serving IP Group, then all calls originating from this Source IP Group are sent to the Serving IP Group. In this scenario, this table is used only if the parameter PreferRouteTable is set to 1.
Web: Destination Prefix EMS: Prefix	Destination (called) telephone number prefix. An asterisk (*) represents any number.
Web/EMS: Source Prefix	Source (calling) telephone number prefix. An asterisk (*) represents any number.
Web/EMS: Source IP Address	Source IP address of the caller (obtained from the Contact header in the INVITE message). **Notes:** ▪ This parameter is applicable only to the Number Manipulation tables for IP-to-Tel calls. ▪ 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. ▪ 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.
Web: Stripped Digits From Left EMS: Number Of Stripped Digits	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	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	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
Web: Suffix to Add EMS: Prefix/Suffix To Add	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	The number of digits that you want to retain 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: Presentation EMS: Is Presentation Restricted	Determines whether Caller ID is permitted: ▪ Not Configured = Privacy is determined according to the Caller ID table (see "Configuring Caller Display Information" on page 155). ▪ **[0]** Allowed = Sends Caller ID information when a call is made using these destination/source prefixes. ▪ **[1]** Restricted = Restricts Caller ID information for these prefixes. **Notes:** ▪ This field is applicable only to Number Manipulation tables for Tel-to-IP source number manipulation. ▪ If 'Presentation' is set to 'Restricted' and the AssertedIdMode parameter is set to 'P-Asserted', the From header in the INVITE message includes the following: From: 'anonymous' <sip: anonymous@anonymous.invalid> and 'privacy: id' header.

3.3.2.8.2.3 Configuring Redirect Number Tel to IP

The 'Redirect Number Tel > IP' page allow you to configure Tel-to-IP Redirect Number manipulation rules. This feature manipulates the prefix of the redirect number received from the PSTN for the outgoing SIP Diversion, Resource-Priority, or History-Info header that is sent to IP.

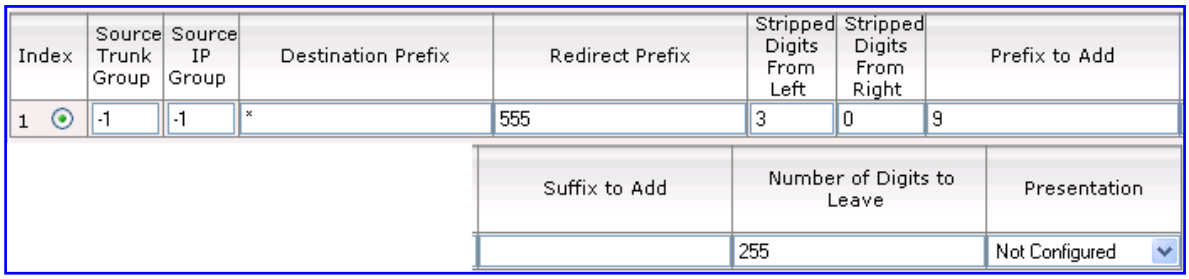
Notes:

- Redirect Tel-to-IP manipulation is not done if the device copies the received destination number to the outgoing SIP redirect number, as enabled by the CopyDest2RedirectNumber parameter.
- You can also configure the Redirect Number Tel to IP table using the *ini* file parameter RedirectNumberMapTel2Ip (see "Number Manipulation and Routing Parameters" on page 474).
- If the characteristics Destination Prefix, Redirect Prefix, and/or Source Address match the incoming SIP message, manipulation is performed according to the configured manipulation rule.
- The manipulation rules are executed 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 Destination Number and Redirect Prefix parameters are used before any manipulation has been done on them.

➢ **To configure redirect Tel-to-IP manipulation rules:**

1. Open the 'Redirect Number Tel > IP' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP submenu** > **Manipulations** submenu > **Redirect Number Tel > IP**).

Figure 3-83: Redirect Number Tel to IP Page



The figure below shows an example configuration in which the redirect prefix "555" is manipulated. According to the configured rule, if for example the number 5551234 is received, after manipulation the device sends the number to IP as 91234.

2. Configure the redirect number Tel to IP rules according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

Table 3-22: Redirect Number Tel to IP Parameters Description

Parameter	Description
Source Trunk Group	The Hunt Group from where the Tel call is received. To denote any Hunt Group, leave this field empty. **Note:** The value -1 indicates that this field is ignored in the rule.
Source IP Group	The IP Group from where the IP-to-IP call originated. Typically, the IP Group of an incoming INVITE is determined/classified using the 'IP to Hunt Group Routing Table'. If not used (i.e., any IP Group), simply leave the field empty. **Notes:** ▪ The value -1 indicates that it is ignored in the rule. ▪ This parameter is applicable only to the IP-to-IP application.
Web/EMS: Destination Prefix	Destination (called) telephone number prefix. An asterisk (*) represents any number.
Web/EMS: Redirect Prefix	Redirect telephone number prefix. An asterisk (*) represents any number.
Web: Stripped Digits From Left EMS: Remove From Left	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: Remove From Right	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/EMS: Prefix to Add	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.
Web/EMS: Suffix to Add	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.

Parameter	Description
Web/EMS: Number of Digits to Leave	The number of digits that you want to retain from the right of the phone number.
Web: Presentation EMS: Is Presentation Restricted	Determines whether Caller ID is permitted: ▪ Not Configured = Privacy is determined according to the Caller ID table (see "Configuring Caller Display Information" on page 155). ▪ **[0]** Allowed = Sends Caller ID information when a call is made using these destination/source prefixes. ▪ **[1]** Restricted = Restricts Caller ID information for these prefixes. **Note:** If 'Presentation' is set to 'Restricted' and the AssertedIdMode parameter is set to 'P-Asserted', then the From header in the INVITE message includes the following: From: 'anonymous' <sip: anonymous@anonymous.invalid> and 'privacy: id' header.

3.3.2.8.2.4 Mapping NPI/TON to SIP Phone-Context

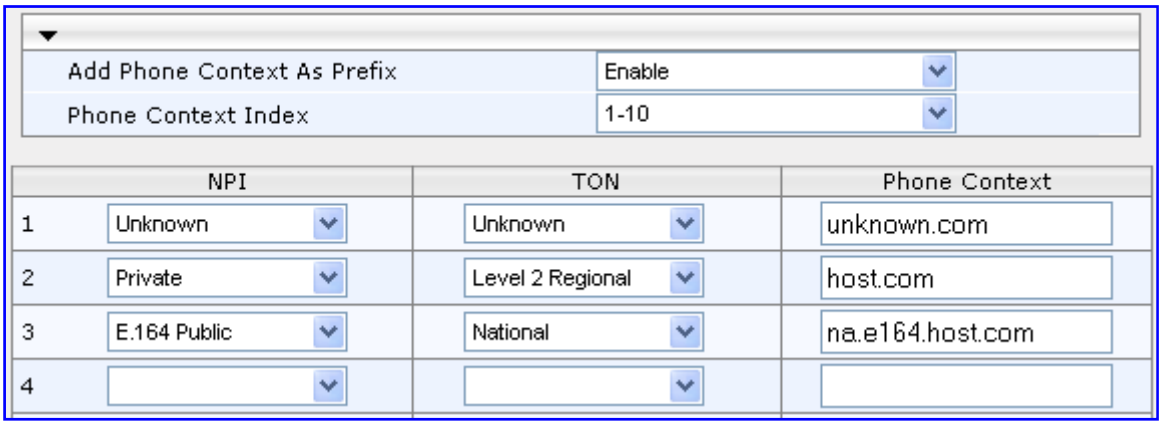
The 'Phone-Context Table' page allows you to map Numbering Plan Indication (NPI) and Type of Number (TON) to the SIP Phone-Context parameter. When a call is received from the Tel, the NPI and TON are compared against the table and the matching Phone-Context value is used in the outgoing SIP INVITE message. The same mapping occurs when an INVITE with a Phone-Context attribute is received. The Phone-Context parameter appears in the standard SIP headers where a phone number is used (Request-URI, To, From, Diversion).

For example, for a Tel-to-IP call with NPI/TON set as E164 National (values 1/2), the device sends the outgoing SIP INVITE URI with the following settings: “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 the Phone-Context tables:**

1. Open the 'Phone Context Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP submenu** > **Manipulations** submenu > **Phone Context**).

Figure 3-84: Phone Context Table Page



2. Configure the Phone Context table according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

Notes:

- Several rows with the same NPI-TON or Phone-Context are allowed. In such a scenario, a Tel-to-IP call uses the first match.
- You can also configure the Phone Context table using the *ini* file table parameter PhoneContext (see "Number Manipulation and Routing Parameters" on page 474).

Table 3-23: Phone-Context Parameters Description

Parameter	Description
Add Phone Context As Prefix **[AddPhoneContextAsPrefix]**	Determines whether the received Phone-Context parameter is added as a prefix to the outgoing Called and Calling numbers. ▪ **[0]** Disable (default) ▪ **[1]** Enable
NPI	Select the Number Plan assigned to this entry. ▪ **[0]** Unknown (default) ▪ **[1]** E.164 Public ▪ **[9]** Private
TON	Select the Type of Number assigned to this entry. ▪ If you selected Unknown as the NPI, you can select Unknown **[0]**. ▪ If you selected Private as the NPI, you can select one of the following: ✓ **[0]** Unknown ✓ **[1]** Level 2 Regional ✓ **[2]** Level 1 Regional ✓ **[3]** PSTN Specific ✓ **[4]** Level 0 Regional (Local) ▪ If you selected E.164 Public as the NPI, you can select one of the following: ✓ **[0]** Unknown ✓ **[1]** International ✓ **[2]** National ✓ **[3]** Network Specific ✓ **[4]** Subscriber ✓ **[6]** Abbreviated
Phone Context	The Phone-Context SIP URI parameter.

3.3.2.8.3 Routing

The **Routing** submenu allows you to configure call routing rules. This submenu includes the following page items:

- General Parameters (see "Configuring General Routing Parameters" on page 137)
- Tel to IP Routing (see "Configuring Tel to IP Routing" on page 138)
- IP to Trunk Group Routing (see "Configuring IP to Hunt Group Routing Table" on page 142)
- Alternative Routing Reasons (see "Configuring Alternative Routing Reasons" on page 144)
- Forward on Busy Trunk (see "Configuring Call Forward upon Busy Trunk" on page 146)

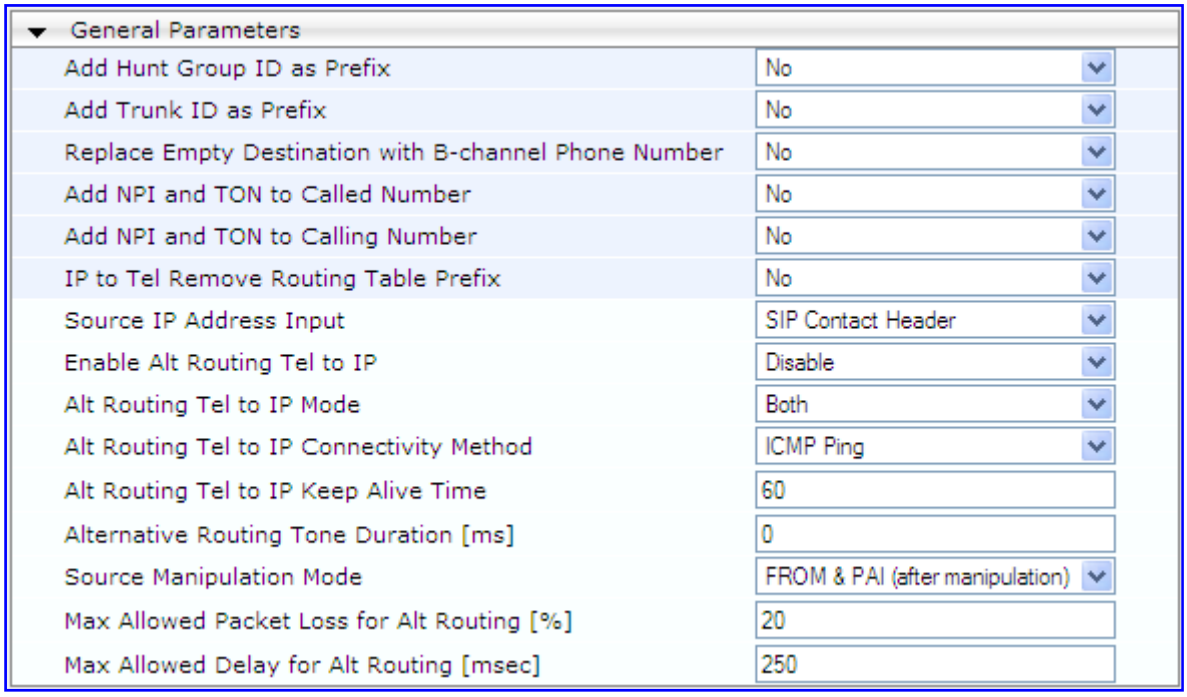
3.3.2.8.3.1 Configuring General Routing Parameters

The 'Routing General Parameters' page allows you to configure general routing parameters. For a description of these parameters, see "Configuration Parameters Reference" on page 333.

➢ **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**).

Figure 3-85: Routing General Parameters Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.8.3.2 Configuring Tel to IP Routing

The 'Tel to IP Routing' page allows you to configure up to 50 Tel-to-IP call routing rules. The device uses these rules to route calls (from the Tel) to IP destinations.

This table provides two main areas for defining a routing rule:

- **Matching Characteristics:** User-defined 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 such as Hunt Group (from where the call is received), source (calling)/destination (called) telephone number prefix.
- **Destination:** User-defined IP destination. If the call matches the characteristics, the device routes the call to this destination. If the number dialed does not match the characteristics, the call is not made. The destination can be any of the following:
  - IP address
  - Fully Qualified Domain Name (FQDN)
  - E.164 Number Mapping (ENUM)
  - Lightweight Directory Access Protocol (LDAP) - for a description, see Routing Based on LDAP Active Directory Queries
  - IP Group - the call is routed to the Proxy Set (IP address) associated with the IP Group (defined in "Configuring IP Groups" on page 103)

When using a proxy server, you don't need to configure this table unless you require one of the following:

- Fallback routing if communication is lost with the proxy server.
- IP Security feature (enabled using the SecureCallFromIP parameter): the device routes only received calls whose source IP address is defined in this table.
- 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.

Note: 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.

Possible uses for configuring routing rules in this table (in addition to those listed above when using a proxy), include the following:

- **Call Restriction:** Rejects calls whose routing rule is associated with the destination IP address 0.0.0.0.
- **Always Use Routing Table feature:** Even if a proxy server is used, the SIP Request-URI host name in the sent 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.
- **Assign 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 specific calls. 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. The call is sent to the alternative destination when one of the following occurs:

- Ping to the initial destination is unavailable, poor QoS (delay or packet loss, calculated according to previous calls) is detected, or a DNS host name is unresolved. For detailed information on Alternative Routing, see "Configuring Alternative Routing (Based on Connectivity and QoS" on page 247).
- A defined Release Reason code (see "Configuring Alternative Routing Reasons" on page 144) is received.

Alternative routing is typically implemented when there is no response to an INVITE message (after INVITE re-transmissions). The device then issues an internal 408 'No Response' implicit Release Reason. If this reason is defined (see "Configuring Alternative Routing Reasons" on page 144), the device immediately initiates a call to the alternative destination using the next matching entry in this routing table. Note that if a domain name in this table is resolved into two IP addresses, the timeout for INVITE re-transmissions can be reduced by using the HotSwapRtx parameter.

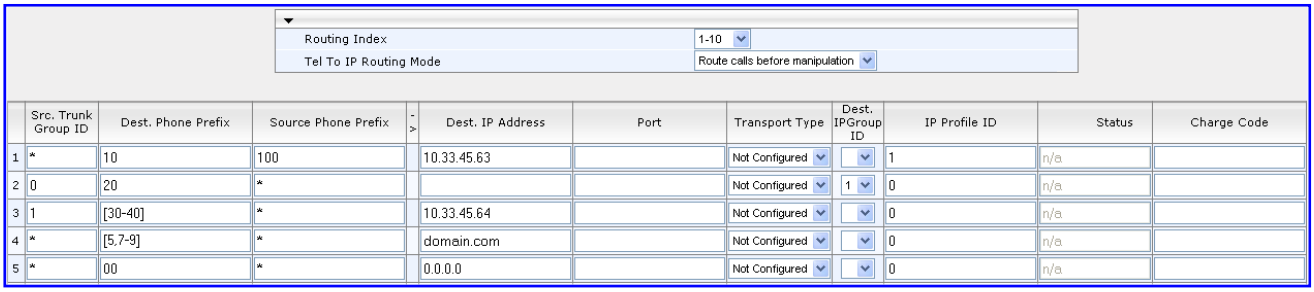
Notes:

- If the alternative routing destination is the device itself, the call can be configured to be routed to the PSTN. This feature is referred to as *PSTN Fallback*. For example, if poor voice quality occurs over the IP network, the call is rerouted through the legacy telephony system (PSTN).
- Outbound IP routing can be performed before or after number manipulation. This is configured using the RouteModeTel2IP parameter, as described below.
- You can also configure this table using the *ini* file table parameter Prefix (see "Number Manipulation and Routing Parameters" on page 474).

➢ **To configure Tel-to-IP routing rules:**

1. Open the 'Tel to IP Routing' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP submenu** > **Routing** submenu > **Tel to IP Routing**).

Figure 3-86: Tel to IP Routing Page



The figure above displays the following Tel-to-IP routing rules:

- **Rule 1:** If the called phone number prefix is 10 and the caller's phone number prefix is 100, the call is assigned settings configured for IP Profile ID 1 and then sent to IP address 10.33.45.63.
- **Rule 2:** For all callers (*), if the called phone number prefix is 20, the call is sent to the destination according to IP Group 1 (which in turn is associated with a Proxy Set ID providing the IP address).
- **Rule 3:** If the called phone number prefix is 5, 7, 8, or 9 and the caller belongs to Hunt Group ID 1, the call is sent to domain.com.
- **Rule 4:** For all callers (*), if the called phone number prefix is 00, the call is rejected (discarded).
- **Rule 5:** For all callers (*), if the called phone number prefix is 6, the call is sent to SRD 2 (i.e., Proxy Set associated with this SRD).

2. From the 'Routing Index' drop-down list, select the range of entries that you want to add.
3. Configure the routing rules according to the table below.
4. Click the **Submit** button to apply your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.

Table 3-24: Tel-to-IP Routing Table Parameters

Parameter	Description
Web/EMS: Tel to IP Routing Mode **[RouteModeTel2IP]**	Determines whether to route received calls to an IP destination before or after manipulation of the destination number. ▪ **[0]** Route calls before manipulation = Calls are routed before the number manipulation rules are applied (default). ▪ **[1]** Route calls after manipulation = Calls are routed after the number manipulation rules are applied. **Notes:** ▪ This parameter is not applicable if outbound proxy routing is used. ▪ For number manipulation, see "Configuring Number Manipulation Tables" on page 129.
Web: Src. Trunk Group ID EMS: Source Trunk Group ID	The Hunt Group from where call is received. **Note:** To denote any Hunt Group, use the asterisk (*) symbol.
Web: Dest. Phone Prefix EMS: Destination Phone Prefix	Prefix of the called telephone number. The prefix can include up to 50 digits. **Note:** To denote any prefix, enter an asterisk (*) symbol. 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 228.
Web/EMS: Source Phone Prefix	Prefix of the calling telephone number. The prefix can include up to 50 digits. **Note:** To denote any prefix, enter an asterisk (*) symbol. 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 228.
All calls matching all or any combination of the above characteristics are sent to the IP destination defined below. **Note:** For alternative routing, additional entries of the same prefix can be configured.	
Web: Dest. IP Address EMS: Address	Destination IP address (in dotted-decimal notation or FQDN) to where the call must be sent. If an FQDN is used (e.g., domain.com), DNS resolution is done according to the DNSQueryType parameter. **Notes:** ▪ If you defined a destination IP Group (below), then this IP address is not used for routing and therefore, not required. ▪ To reject calls, enter 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. ▪ For routing calls between phones connected to the device (i.e., local routing), enter the device's IP address. ▪ When the device's IP address is unknown (e.g., when DHCP is used), enter IP address 127.0.0.1. ▪ When using domain names, you must enter the DNS server's IP address or alternatively, define these names in the 'Internal DNS Table' (see "Configuring the Internal DNS Table" on page 87).

Parameter	Description
	▪ If the string 'ENUM' is specified for the destination IP address, an ENUM query containing the destination phone number is sent to the DNS server. The ENUM reply includes a SIP URI used as the Request-URI in the outgoing INVITE and for routing (if a proxy is not used). ▪ The IP address can include the following wildcards: ✓ "x": represents single digits. For example, 10.8.8.xx depicts all addresses between 10.8.8.10 and 10.8.8.99. ✓ "*": represents any number between 0 and 255. For example, 10.8.8.* depicts all addresses between 10.8.8.0 and 10.8.8.255.
Web: Port EMS: Destination Port	The destination port to where you want to route the call.
Web/EMS: Transport Type	The transport layer type used for sending the IP call: ▪ **[-1]** Not Configured ▪ **[0]** UDP ▪ **[1]** TCP ▪ **[2]** TLS **Note:** When set to Not Configured (-1), the transport type defined by the SIPTransportType parameter is used.
Web: Dest IP Group ID EMS: Destination IP Group ID	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. **Notes:** ▪ 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). ▪ If the parameter AlwaysUseRouteTable is set to 1 (see "Configuring IP Groups" on page 103), 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). ▪ 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 113). ▪ For defining Proxy Set ID's, see "Configuring Proxy Sets Table" on page 106.
IP Profile ID	IP Profile ID (see "Configuring IP Profiles" on page 122) assigned to this IP destination call. This allows you to assign numerous configuration attributes (e.g., voice codes) per routing rule.
Status	Read-only field displaying the Quality of Service of the destination IP address: ▪ n/a = Alternative Routing feature is disabled. ▪ OK = IP route is available. ▪ Ping Error = No ping to IP destination; route is unavailable. ▪ QoS Low = Poor QoS of IP destination; route is unavailable. ▪ DNS Error = No DNS resolution (only when domain name is used instead of an IP address).

Parameter	Description
Web/EMS: Charge Code	Optional Charge Code assigned to the routing rule. For configuring Charge Codes, see Configuring Charge Codes Table on page 151. **Note:** This parameter is applicable only to FXS interfaces.

3.3.2.8.3.3 Configuring IP to Hunt Group Routing Table

The 'IP to Hunt Group Routing Table' page allows you to configure up to 24 inbound (IP-to-Tel / Hunt Group) call routing rules. The specific channel pertaining to the Hunt Group to which the call is routed is determined according to the Hunt Group's channel selection mode. The channel selection mode can be defined per Hunt Group (see "Configuring Hunt Group Settings" on page 126), or for all Hunt Groups using the global parameter ChannelSelectMode.

This table provides two main areas for defining a routing rule:

- **Matching Characteristics:** user-defined characteristics of the incoming IP call are defined in this area. If the characteristics match a table entry, the rule is used to route the call. One or more characteristics can be defined for the rule such as source (calling)/destination (called) telephone number prefix, and source IP address (from where call received).
- **Destination:** user-defined destination. If the call matches the characteristics, the device routes the call to this destination. The destination is a selected Hunt Group.

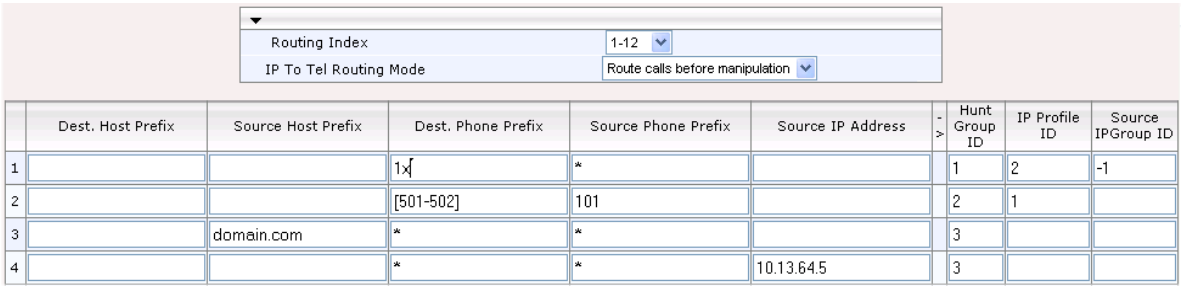
Notes:

- When a call release reason (defined in "Configuring Reasons for Alternative Routing" on page 144) is received for a specific IP-to-Tel call, an alternative Hunt Group for that call can be configured. This is done by configuring an additional routing rule for the same call characteristics, but with a different Hunt Group ID.
- You can also configure the 'IP to Hunt Group Routing Table' using the *ini* file table parameter PSTNPrefix (see "Number Manipulation and Routing Parameters" on page 474).

➢ **To configure IP-to-Tel routing rules:**

1. Open the 'IP to Hunt Group Routing Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** submenu > **IP to Trunk Group Routing**).

Figure 3-87: Inbound IP Routing Table Page



The above 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 Hunt 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 Hunt Group ID 2.
- **Rule 3:** If the incoming IP call has a From URI host prefix as domain.com, the call is routed to Hunt Group ID 3.

2. From the 'Routing Index' drop-down list, select the range of entries that you want to add.
3. Configure the inbound IP routing rule according to the table below.
4. Click the **Submit** button to save your changes.
5. To save the changes so they are available after a power failure, see "Saving Configuration" on page 169.

Table 3-25: IP-to-Tel Routing Table Description

Parameter	Description
IP to Tel Routing Mode **[RouteModeIP2Tel]**	Determines whether to route the incoming IP call before or after manipulation of destination number (configured in "Configuring Number Manipulation Tables" on page 129). ▪ **[0]** Route calls before manipulation = Incoming IP calls are routed before number manipulation (default). ▪ **[1]** Route calls after manipulation = Incoming IP calls are routed after number manipulation are applied.
Dest. Host Prefix	The Request-URI host name prefix of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty. **Note:** The asterisk (*) wildcard can be used to depict any prefix.
Source Host Prefix	The From URI host name prefix of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty. **Notes:** ▪ The asterisk (*) wildcard can be used to depict any prefix. ▪ 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).
Dest. Phone Prefix	The called telephone number prefix. The prefix can include up to 49 digits. **Note:** The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 228.
Source Phone Prefix	The calling telephone number prefix. The prefix can include up to 49 digits. **Note:** The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 228.

Parameter	Description
Source IP Address	The source IP address of the incoming IP call (obtained from the Contact header in the INVITE message) that can be used for routing decisions. **Notes:** ▪ You can configure from where the source IP address is obtained, using the parameter SourceIPAddressInput. ▪ The source IP address can include the following wildcards: ✓ "x": depicts single digits. For example, 10.8.8.xx represents all the addresses between 10.8.8.10 and 10.8.8.99. ✓ "*": depicts any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255.
Calls matching all or any combination of the above characteristics are sent to the Hunt Group ID defined below. **Note:** For alternative routing, additional entries of the same characteristics can be configured.	
Hunt Group ID	The Hunt Group to which the incoming SIP call is assigned if it matches all or any combination of the parameters described above.
IP Profile ID	The IP Profile (configured in "Configuring IP Profiles" on page 122) to assign to the call.
Source IP Group ID	The IP Group associated with the incoming IP call. This is the IP Group from where the INVITE message originated. 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 113).

3.3.2.8.3.4 Configuring Alternative Routing Reasons

The 'Reasons for Alternative Routing' page allows you to define up to five Release Reason codes for IP-to-Tel and Tel-to-IP call failure reasons. If a call is released as a result of one of these reasons, the device tries to find an alternative route for the call. The device supports up to two different alternative routes.

The release reasons depend on the call direction:

- **Release reason for IP-to-Tel calls:** Reason for call release on the Tel side, provided in Q.931 notation. As a result of a release reason, an alternative Hunt Group is provided. For defining an alternative Hunt Group, see "Configuring IP to Hunt Group Routing Table" on page 142. This call release reason type can be configured, for example, when the destination is busy and release reason #17 is issued or for other call releases that issue the default release reason (#3) - see the parameter DefaultReleaseCause.
- **Release reason for Tel-to-IP calls:** Reason for call release on the IP side, provided in SIP 4xx, 5xx, and 6xx response codes. As a result of a release reason, an alternative IP address is provided. For defining an alternative IP address, see "Configuring Tel to IP Routing" on page 138. This call release reason type can be configured, for example, when there is no response to an INVITE message (after INVITE re-transmissions), the device issues an internal 408 'No Response' implicit release reason.

The device 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.

Notes:

- To enable alternative routing using the IP-to-Tel routing table, set the parameter RedundantRoutingMode to 1 (default).
- The reasons for alternative routing for Tel-to-IP calls also apply for Proxies (if the parameter RedundantRoutingMode is set to 2).
- You can also configure alternative routing using the *ini* file table parameters AltRouteCauseTel2IP and AltRouteCauseIP2Tel (see "Number Manipulation and Routing Parameters" on page 474).

➢ **To configure reasons for alternative routing:**

1. Open the 'Reasons for Alternative Routing' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** submenu > **Alternative Routing Reasons**).

Figure 3-88: Reasons for Alternative Routing Page

2. In the 'IP to Tel Reasons' group, select up to five different call failure reasons that invoke an alternative IP-to-Tel routing.
3. In the 'Tel to IP Reasons' group, select up to five different call failure reasons that invoke an alternative Tel-to-IP routing.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.8.3.5 Configuring Call Forward upon Busy Trunk

The 'Forward on Busy Trunk Destination' page allows you to configure forwarding of IP-to-Tel calls (call redirection) to a different (alternative) IP destination, using SIP 3xx responses, if an unavailable FXS/FXO Hunt Group exists. This feature can be used, for example, to forward the call to another FXS/FXO device.

This alternative destination is configured per Hunt Group.

The alternative destination can be defined as a host name (IP address with optional port and transport type), 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 or alternative routing fails, and the following reason (included in the SIP Diversion header of 3xx messages) exists:

- "unavailable": All FXS/FXO lines pertaining to a Hunt Group are busy or unavailable

Note: You can also configure the Forward on Busy Trunk Destination table using the *ini* file parameter table ForwardOnBusyTrunkDest.

➢ **To configure the Forward on Busy Trunk Destination rules:**

1. Open the 'Forward on Busy Trunk Destination' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** submenu > **Forward on Busy Trunk**).

Figure 3-89: Forward on Busy Trunk Destination Page

Index	Trunk Group ID	Forward Destination
0	1	10.13.5.67

The figure above displays a configuration that forwards IP-to-Tel calls destined for Hunt 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 the **Submit** button to save your changes.
3. To save the changes so they are available after a power fail, see "Saving Configuration" on page 169.

3.3.2.8.4 DTMF and Supplementary

The **DTMF and Supplementary** submenu allows you to configure DTMF and supplementary parameters. This submenu includes the following page items:

- DTMF & Dialing (see "Configuring DTMF and Dialing" on page 147)
- Supplementary Services (see "Configuring Supplementary Services" on page 148)

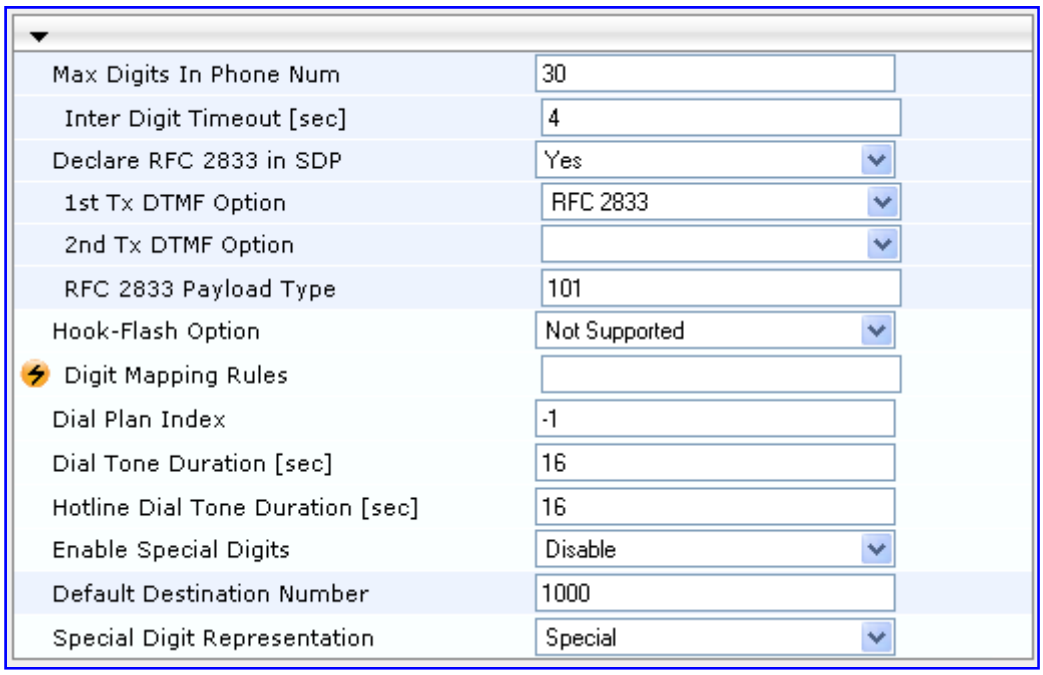
3.3.2.8.4.1 Configuring DTMF and Dialing

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 333.

➢ **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**).

Figure 3-90: DTMF & Dialing Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

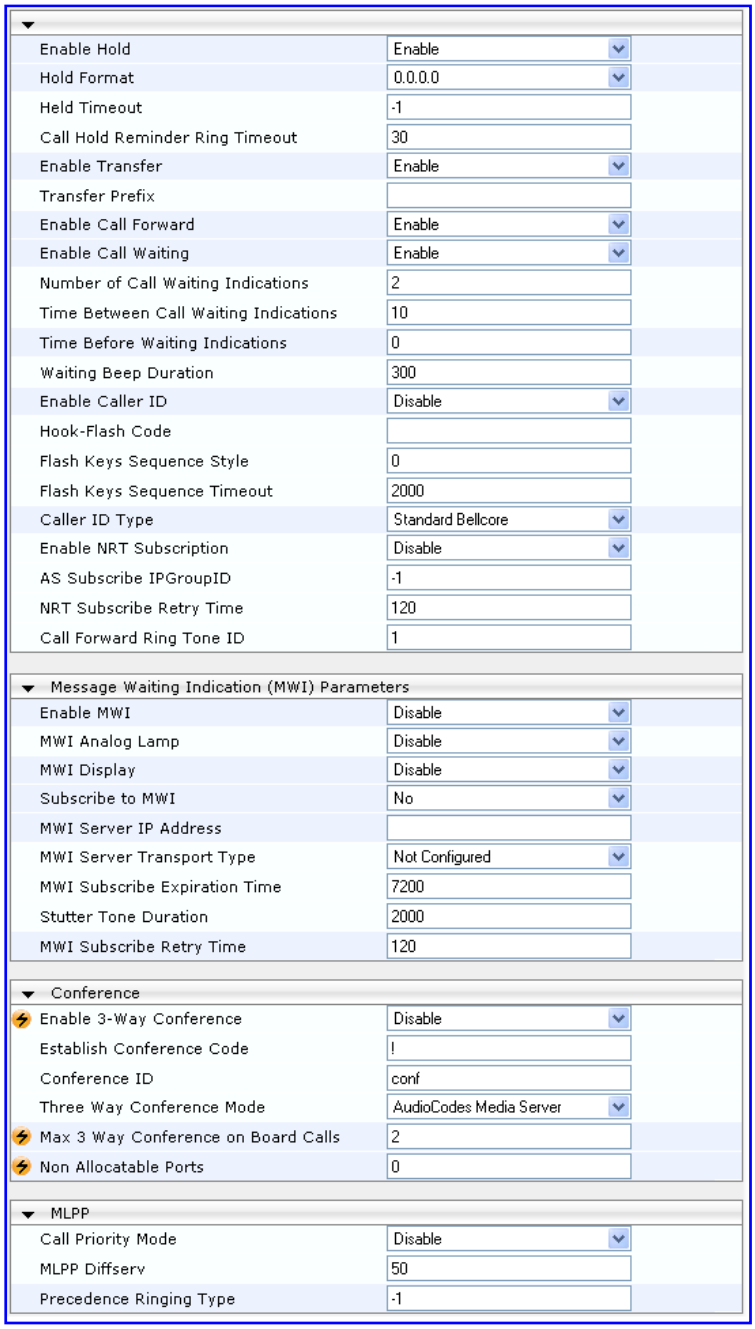
3.3.2.8.4.2 Configuring Supplementary Services

The 'Supplementary Services' page is used to configure parameters associated with supplementary services. For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333. For an overview on supplementary services, see "Working with Supplementary Services" on page 254.

➢ **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 3-91: Supplementary Services Page



2. Configure the parameters as required.

3. Click the **Submit** button to save 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 169.

3.3.2.8.5 Analog Gateway

The **Analog Gateway** submenu allows you to configure analog settings. This submenu includes the following page items:

- Keypad Features (see "Configuring Keypad Features" on page 149)
- Metering Tones (see "Configuring Metering Tones" on page 151)
- Charge Codes (see "Configuring Charge Codes" on page 151)
- FXO Settings (see "Configuring FXO Settings" on page 152)
- Authentication (see "Configuring Authentication" on page 153)
- Automatic Dialing (see "Configuring Automatic Dialing" on page 154)
- Caller Display Information (see "Configuring Caller Display Information" on page 155)
- Call Forward (see "Configuring Call Forward" on page 157)
- Caller ID Permissions (see "Configuring Caller ID Permissions" on page 158)
- Call Waiting (see "Configuring Call Waiting" on page 159)

3.3.2.8.5.1 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 (see "Configuring Call Forward" on page 157)
- Caller ID Restriction (see "Configuring Caller Display Information" on page 155)
- Hotline (see "Configuring Automatic Dialing" on page 154)
- Call Transfer
- Call Waiting (see "Configuring Call Waiting" on page 159)
- Rejection of Anonymous Calls

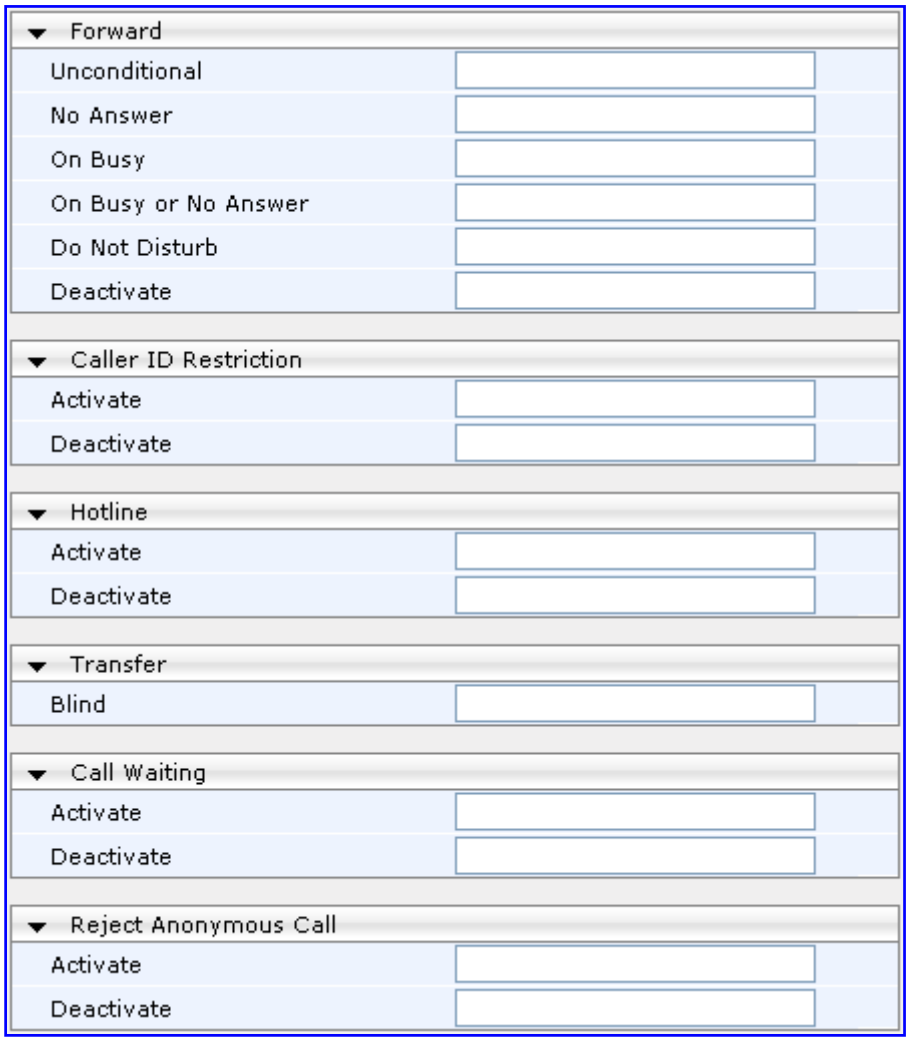
Notes:

- 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).

➢ **To configure the keypad features**

1. Open the 'Keypad Features' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Keypad Features**).

Figure 3-92: Keypad Features Page



2. Configure the keypad features as required. For a description of these parameters, see "Configuration Parameters Reference" on page 333.
3. Click the **Submit** button to save your changes.
4. To save the changes to the flash memory, see "Saving Configuration" on page 169.

3.3.2.8.5.2 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.

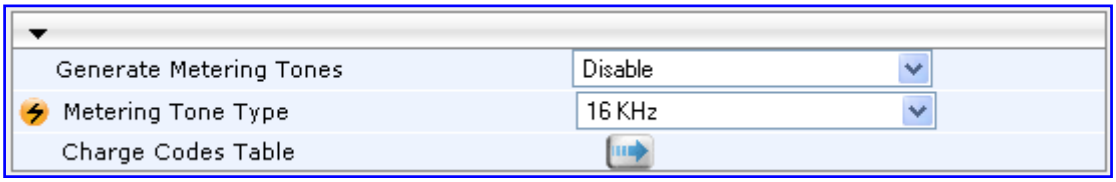
Notes:

- The 'Metering Tones' page is available only for FXS interfaces.
- Charge Code rules can be assigned to routing rules in the 'Tel to IP Routing' (see "Configuring Tel to IP Routing" on page 138). When a new call is established, the 'Tel to IP Routing' 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** submenu > **Analog Gateway** submenu > **Metering Tones**).

Figure 3-93: Metering Tones Page



2. Configure the Metering tones parameters as required. For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 333.
3. Click the **Submit** button to save your changes.
4. To save the changes to the flash memory, see "Saving Configuration" on page 169.

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 a detailed description on configuring the Charge Codes table, see "Configuring Charge Codes Table" on page 151.

3.3.2.8.5.3 Configuring Charge Codes

The 'Charge Codes Table' page 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 'Tel to IP Routing'.

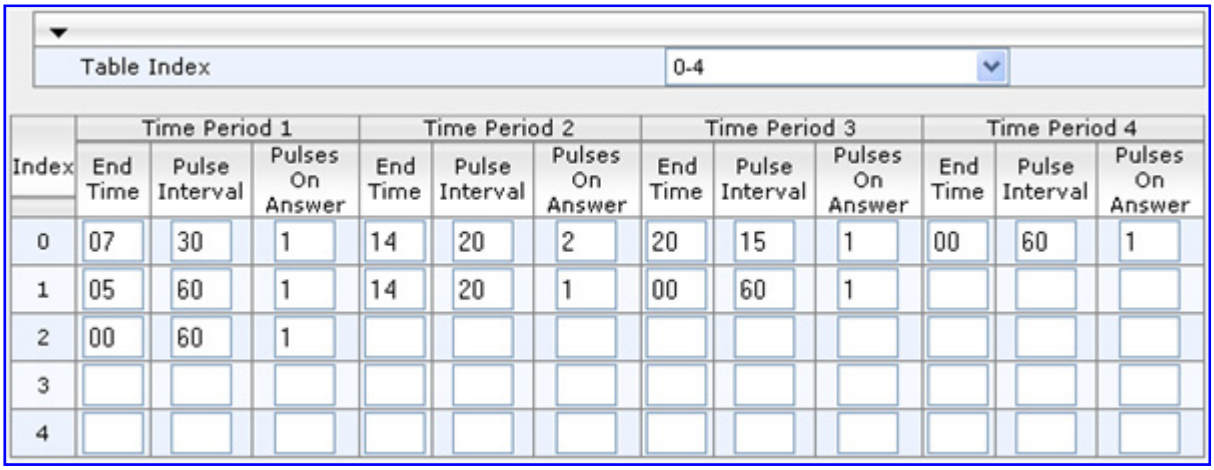
Notes:

- The 'Charge Codes Table' page is available only for FXS interfaces.
- You can also configure the Charge Codes table using the *ini* file table parameter ChargeCode.

➢ **To configure the Charge Codes:**

1. Access 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 151).

Figure 3-94: Charge Codes Table Page



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. Define up to 25 different charge codes (each charge code is defined per row). Each charge code can include up to four different time periods in a day (24 hours). Each time period is composed of the following:
   - The end of the time period (in a 24 rounded-hour's format).
   - The time interval between pulses (in tenths of a second).
   - The number of pulses sent on answer.

   The first time period always starts at midnight (00). It is mandatory that the last time period of each rule ends at midnight (00). This prevents undefined time frames in a day. 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.
3. Click the **Submit** button to save your changes.
4. To save the changes to the flash memory, see "Saving Configuration" on page 169.

3.3.2.8.5.4 Configuring FXO Settings

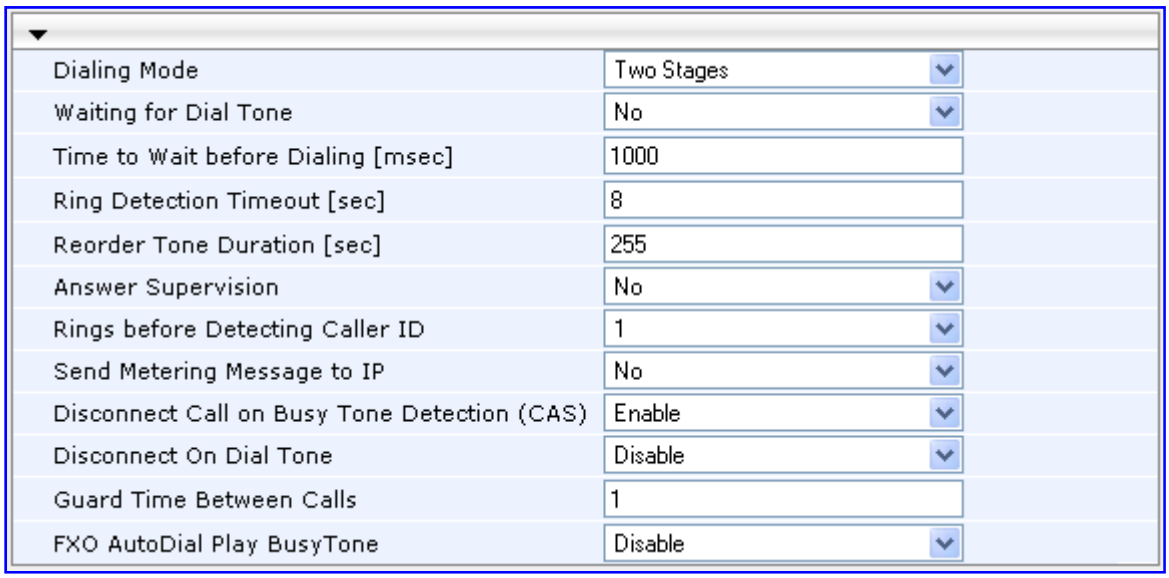
The 'FXO Settings' page allows you to configure the device's specific FXO parameters. For a description of these parameters, see "Configuration Parameters Reference" on page 333.

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** submenu > **Analog Gateway** submenu > **FXO Settings**).

Figure 3-95: FXO Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.8.5.5 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 performed per port or for the entire device, use the parameter AuthenticationMode. If authentication is for the entire device, the configuration on this page is ignored.
- If either the user name or password fields are omitted, the port's phone number and global password (using the Password parameter) are used instead.
- After you click the **Submit** button, the password is displayed as an asterisk (*).
- You can also configure Authentication using the *ini* file table parameter Authentication (see SIP Configuration Parameters).

➢ **To configure the Authentication Table:**

1. Set the parameter 'Authentication Mode' (AuthenticationMode) to 'Per Endpoint'.
2. Open the 'Authentication' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Authentication**).

Gateway Port	User Name	Password
Port 1 FXS		
Port 2 FXS		
Port 3 FXS		
Port 4 FXS		
Port 5 FXO		
Port 6 FXO		
Port 7 FXO		
Port 8 FXO		

3. In the 'User Name' and 'Password' fields corresponding to a port, enter the user name and password respectively.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.8.5.6 Configuring Automatic Dialing

The 'Automatic Dialing' page allows you to define a telephone number that is automatically dialed when an FXS or FXO port is used (e.g., off-hooked).

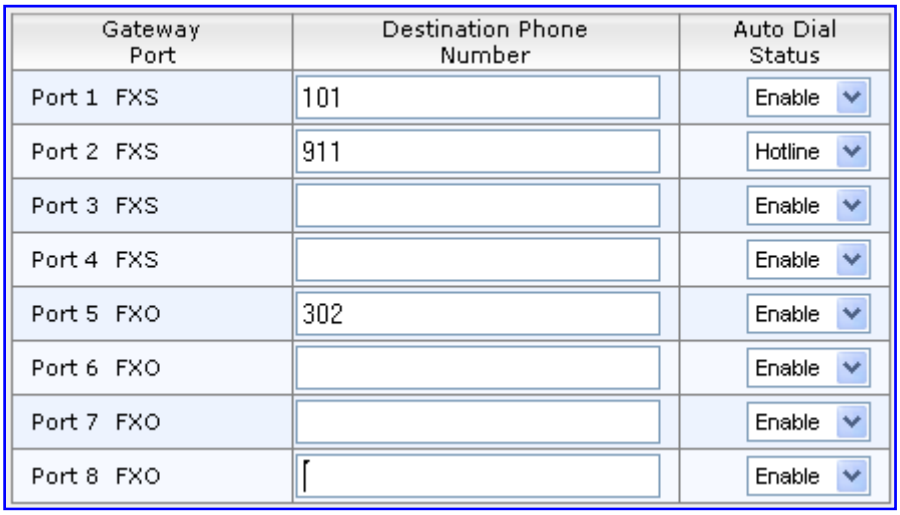
Notes:

- After a ring signal is detected on an 'Enabled' FXO port, the device initiates a call to the destination number without seizing the line. The line is seized only after the call is answered.
- After a ring signal is detected on a 'Disabled' or 'Hotline' FXO port, the device seizes the line.
- You can also configure automatic dialing using the *ini* file table parameter TargetOfChannel.
- You can configure the device to play a Busy/Reorder tone to the Tel side upon receiving a SIP 4xx, 5xx, or 6xx response from the IP side (i.e., Tel-to-IP call failure), using the *ini* file parameter FXOAutoDialPlayBusyTone (see SIP Configuration Parameters).

➢ **To configure Automatic Dialing:**

1. Open the 'Automatic Dialing' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Automatic Dialing**).

Figure 3-96: Automatic Dialing Page



2. In the 'Destination Phone Number' field corresponding to a port, enter the telephone number that you want automatically dialed.
3. From the 'Auto Dial Status' drop-down list, select one of the following:
   - Disable **[0]**: The automatic dialing feature for the specific port is disabled (i.e., the number in the 'Destination Phone Number' field is ignored).
   - Enable **[1]**: The number in the 'Destination Phone Number' field is automatically dialed if the phone is off-hooked (for FXS interfaces) or a ring signal (from PBX/PSTN switch) is detected (FXO interfaces). The FXO line is seized only after the SIP call is answered.
   - Hotline **[2]**:
     - **FXS interfaces:** When a phone is off-hooked and no digit is dialed for a user-defined time (configured using the parameter HotLineToneDuration), the number in the 'Destination Phone Number' field is automatically dialed.
     - **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 for a user-defined time (configured using the parameter HotLineToneDuration), the number in the 'Destination Phone Number' field is automatically dialed by sending a SIP INVITE message with this number.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.8.5.7 Configuring Caller Display Information

The 'Caller Display Information' page allows you to enable the device to send Caller ID information to IP when a call is made. The called party can use this information for caller identification. The information configured on this page is sent in an INVITE message in the From header. For information on Caller ID restriction according to destination/source prefixes, see "Configuring Number Manipulation Tables" on page 129.

Notes:

- When FXS ports receive 'Private' or 'Anonymous' strings in the From header, they don't send the calling name or number to the Caller ID display.
- If Caller ID name is detected on an FXO line (EnableCallerID = 1), it is used instead of the Caller ID name defined on this page.
- When the 'Presentation' field is set to 'Restricted', the Caller ID is sent to the remote side using only the P-Asserted-Identity and P-Preferred-Identity headers (AssertedIdMode).
- To maintain backward compatibility, when the strings 'Private' or 'Anonymous' are entered 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 can be overridden by configuring the 'Presentation' field in the 'Source Number Manipulation' table (see "Configuring Number Manipulation Tables" on page 129).
- You can also configure the Caller Display Information table using the *ini* file table parameter CallerDisplayInfo.

➢ **To configure the Caller Display Information:**

1. Open the 'Caller Display Information' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Caller Display Information**).

Figure 3-97: Caller Display Information Page

Gateway Port	Caller ID/Name	Presentation
Port 1 FXS	Private	Restricted
Port 2 FXS	Susan C.	Restricted
Port 3 FXS	Lee P.	Allowed
Port 4 FXS	Ronaldino E.	Restricted
Port 5 FXO	Hung L.	Allowed
Port 6 FXO		Allowed
Port 7 FXO		Allowed
Port 8 FXO		Allowed

2. In the 'Caller ID/Name' field corresponding to the desired port, enter the Caller ID string (up to 18 characters).
3. From the 'Presentation' drop-down list, select one of the following:
   - 'Allowed' **[0]** - sends the string defined in the 'Caller ID/Name' field when a Tel-to-IP call is made using the corresponding device port.
   - 'Restricted' **[1]** - the string defined in the 'Caller ID/Name' field is not sent.
4. Click the **Submit** button to save your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.8.5.8 Configuring Call Forward

The 'Call Forwarding Table' page allows you to forward (redirect) IP-to-Tel calls (using SIP 302 response) originally destined to specific device ports, to other device ports or to an IP destination.

Notes:

- Ensure that the Call Forward feature is enabled (default) for the settings on this page to take effect. To enable Call Forward, use the parameter EnableForward ("Configuring Supplementary Services" on page 148).
- You can also configure the Call Forward table using the *ini* file table parameter FwdInfo.

➢ **To configure Call Forward per port:**

1. Open the 'Call Forward Table' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Call Forward**).

Figure 3-98: Call Forward Table Page

Gateway Port	Forward Type	Forward to Phone Number	Time for No Reply Forward
Port 1 FXS	On busy	201	30
Port 2 FXS	On busy	201	30
Port 3 FXS	No Answer	203	30
Port 4 FXS	Unconditional	202@10.2.1.1	30
Port 5 FXO	Deactivate		30

2. Configure the Call Forward parameters for each port according to the table below.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

Table 3-26: Call Forward Table

Parameter	Description
Forward Type	Determines the scenario for forwarding a call. ▪ **[0]** Deactivate = Don't forward incoming calls (default). ▪ **[1]** On Busy = Forward incoming calls when the port is busy. ▪ **[2]** Unconditional = Always forward incoming calls. ▪ **[3]** No Answer = Forward incoming calls that are not answered within the time specified in the 'Time for No Reply Forward' field. ▪ **[4]** 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. ▪ **[5]** Do Not Disturb = Immediately reject incoming calls.
Forward to Phone Number	The telephone number or URI (<number>@<IP address>) to where the call is forwarded. **Note:** If this field only contains a telephone number and a Proxy isn't used, the 'forward to' phone number must be specified in the 'Tel to IP Routing' (see "Configuring Tel to IP Routing" on page 138).

Parameter	Description
Time for No Reply Forward	If you have set the 'Forward Type' for this port to 'No Answer', enter the number of seconds the device waits before forwarding the call to the phone number specified.

3.3.2.8.5.9 Configuring Caller ID Permissions

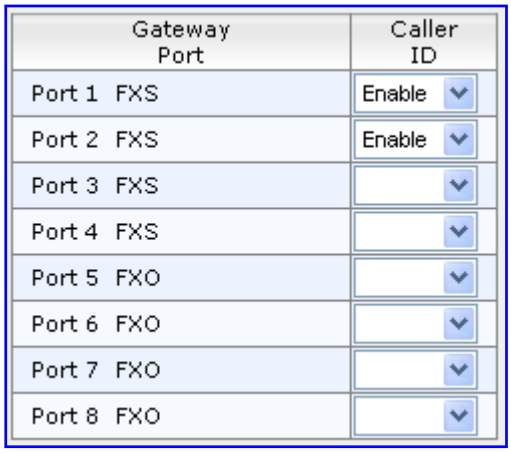
The 'Caller ID Permissions' page allows you to enable or disable (per port) the Caller ID generation (for FXS interfaces) and detection (for FXO interfaces). If a port isn't configured, its Caller ID generation/detection is determined according to the global parameter EnableCallerID described in "Configuring Supplementary Services" on page 148.

Note: You can also configure the Caller ID Permissions table using the *ini* file table parameter EnableCallerID.

➢ **To configure Caller ID Permissions per port:**

1. Open the 'Caller ID Permissions' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Caller ID Permissions**).

Figure 3-99: Caller ID Permissions Page



2. From the 'Caller ID' drop-down list, select one of the following:
   - 'Enable': Enables Caller ID generation (FXS) or detection (FXO) for the specific port.
   - 'Disable': Caller ID generation (FXS) or detection (FXO) for the specific port is disabled.
   - Not defined: Caller ID generation (FXS) or detection (FXO) for the specific port is determined according to the parameter 'Enable Caller ID' (described in "Configuring Supplementary Services" on page 148).
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.8.5.10 Configuring Call Waiting

The 'Call Waiting' page allows you to enable or disable call waiting per device FXS port.

Notes:

- This page is applicable only to FXS interfaces.
- Instead of using this page, you can enable or disable call waiting for all the device's ports, using the global call waiting parameter 'Enable Call Waiting' (see "Configuring Supplementary Services" on page 148).
- You can also configure the Call Waiting table using the *ini* file table parameter CallWaitingPerPort (see SIP Configuration Parameters).
- For additional call waiting configuration, see the following parameters: FirstCallWaitingToneID (in the CPT file), TimeBeforeWaitingIndication, WaitingBeepDuration, TimeBetweenWaitingIndications, and NumberOfWaitingIndications.

➢ **To configure Call Waiting:**

1. Open the 'Caller Waiting' page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Call Waiting**).

Figure 3-100: Call Waiting Page

Gateway Port	Call Waiting Configuration
Port 1 FXS	Enable
Port 2 FXS	
Port 3 FXS	
Port 4 FXS	
Port 5 FXO	

2. From the 'Call Waiting Configuration' drop-down list corresponding to the port you want to configure for call waiting, select one of the following options:
   - 'Enable': Enables call waiting for the specific port. When the device receives a call on a busy endpoint (port), it responds with a 182 response (not with a 486 busy). The device plays a call waiting indication signal. When hook-flash is detected by the device, 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.
   - 'Disable': No call waiting for the specific port.
   - Empty: Call waiting is determined according to the global parameter 'Enable Call Waiting' (described in "Configuring Supplementary Services" on page 148).
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.8.6 Advanced Applications

The **Advanced Applications** menu allows you to configure advanced SIP-based applications. This menu includes the following page item:

- Voice Mail Settings (see "Configuring Voice Mail Parameters" on page 160)

3.3.2.8.6.1 Configuring Voice Mail Parameters

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 333.

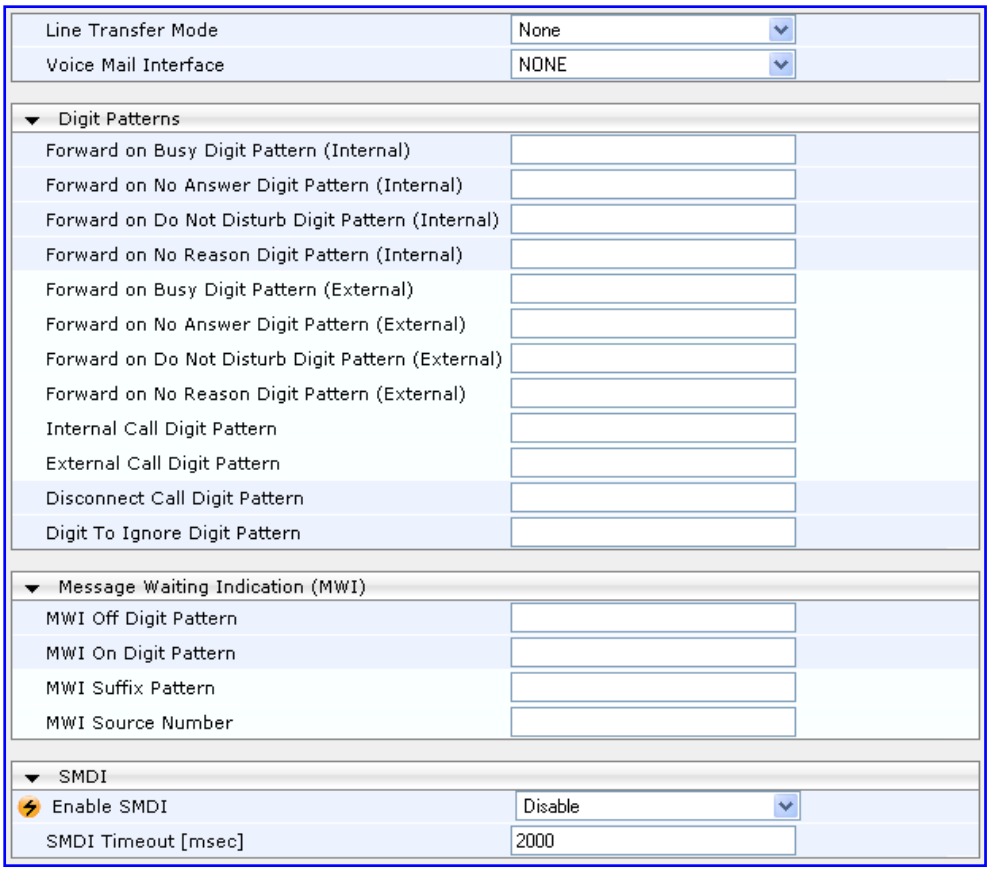
Notes:

- The 'Voice Mail Settings' page is available only for FXO interfaces.
- For detailed information on configuring the voice mail application, 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** submenu > **Advanced Applications** submenu > **Voice Mail Settings**).

Figure 3-101: Voice Mail Settings Page



2. Configure the parameters as required.
3. Click the **Submit** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

3.3.2.9 SAS

The **SAS** submenu allows you to configure the SAS application. This submenu includes the **Stand Alone Survivability** item page (see "Configuring Stand-Alone Survivability" on page 161), from which you can also access the 'IP2IP Routing Table' page for configuring SAS routing rules (see "Configuring IP2IP Routing Table (SAS)" on page 163).

Notes:

- The SAS menu and its page items appear only if you have enabled the SAS application (see "Enabling Applications" on page 102) and the SAS application is included in the device's Software Upgrade Key (see "Loading Software Upgrade Key" on page 172).
- For a detailed explanation on SAS, see "Stand-Alone Survivability (SAS) Application" on page 279.

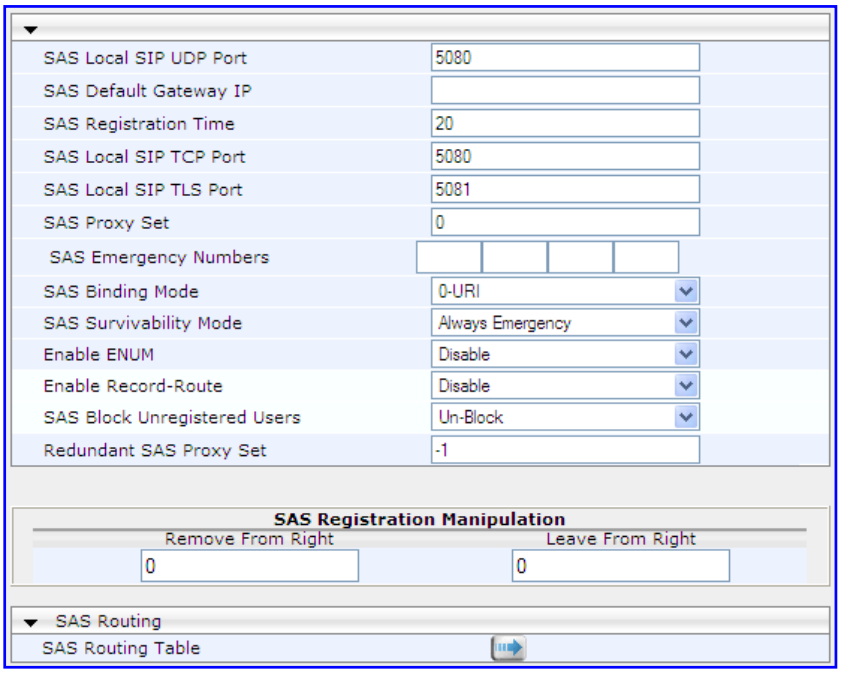
3.3.2.9.1 Configuring Stand-Alone Survivability

The 'SAS Configuration' page allows you to configure the device's Stand-Alone Survivability (SAS) feature. This feature is useful for providing a local backup through the PSTN in Small or Medium Enterprises (SME) that are serviced by IP Centrex services. In such environments, the enterprise's incoming and outgoing telephone calls (external and internal) are controlled by the Proxy, which communicates with the enterprise through the WAN interface. SAS ensures that incoming, outgoing, and internal calls service is maintained in case of WAN or Proxy failure, using a PSTN (or an alternative VoIP) backup connection and the device's internal call routing. To utilize the SAS feature, the VoIP CPEs such as IP phones or residential gateways need to be defined so that their Proxy and Registrar destination addresses and UDP port is the same as the device's SAS IP address and SAS local SIP UDP port.

➢ **To configure SAS:**

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

Figure 3-102: SAS Configuration Page



2. Configure the individual parameters as described in SIP Configuration Parameters.
3. Configure the SAS Registration Manipulation table to manipulate the SIP Request-URI user part of incoming INVITE messages and of incoming REGISTER request AoR (in the To header), before it is saved to the registered users database.
   - **Remove From Right:** Number of digits removed from the right side of the user part before saving to the registered user database.
   - **Leave From Right:** Number of digits to retain from the right side of the user part.

Notes:

- Once manipulated, the SAS application searches for the user in the registration database.
- The SAS Registration Manipulation feature does not modify the Request-URI of the outgoing INVITE message.
- The SAS Registration Manipulation can also be configured using the SASRegistrationManipulation *ini* file parameter (see "SAS Parameters" on page 161).

4. Click the **Submit** button to apply your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 169.
6. To configure the SAS Routing table, under the **SAS Routing** group, click the **SAS Routing Table** button to open the 'IP2IP Routing Table' page. For a description of this table, see "Configuring the IP2IP Routing Table (SAS)" on page 163.

3.3.2.9.2 Configuring IP2IP Routing Table (SAS)

The 'IP2IP 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 IP2IP 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 IP2IP Routing table can also be configured using the *ini* file table parameter IP2IPRouting (see SIP Configuration Parameters).

➢ **To configure the IP2IP Routing table for SAS:**

1. In the 'SAS Configuration' page (see "Configuring Stand-Alone Survivability" on page 161), click the **SAS Routing Table** button; the 'IP2IP Routing Table' page appears.
2. Add an entry and then configure it according to the table below.
3. Click the **Apply** button to save your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 169.

Table 3-27: SAS IP2IP Routing Table Parameters

Parameter	Description
Matching Characteristics	
Source Username Prefix **[IP2IPRouting_SrcUsernamePrefix]**	The prefix of the user part of the incoming INVITE's source URI (usually the From URI). The default is "*". **Note:** The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 228.
Source Host **[IP2IPRouting_SrcHost]**	The host part of the incoming SIP INVITE'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. The default is "*".
Destination Username Prefix **[IP2IPRouting_DestUsernamePrefix]**	The prefix of the incoming SIP INVITE's destination URI (usually the Request URI) user part. If this rule is not required, leave the field empty. To denote any prefix, use the asterisk (*) symbol. The default is "*".

Parameter	Description
Destination Host **[IP2IPRouting_DestHost]**	The host part of the incoming SIP INVITE's destination URI (usually the Request URI). If this rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any destination host. The default is "*".
Request Type **[IP2IPRouting_RequestType]**	The type of incoming SIP request: ▪ **[0]** All (default) ▪ **[1]** INVITE ▪ **[2]** REGISTER ▪ **[3]** SUBSCRIBE ▪ **[4]** INVITE & REGISTER ▪ **[5]** INVITE & SUBSCRIBE
Operation Routing Rule (performed when match found in above characteristics)	
Destination Type **[IP2IPRouting_DestType]**	Determines the destination type to which the outgoing INVITE is sent. ▪ **[0]** IP Group (default) = The INVITE is sent to the IP Group's Proxy Set (if the IP Group is of SERVER type) \ registered contact from the database (if USER type). ▪ **[1]** Dest Address = The INVITE is sent to the address configured in the following fields: 'Destination Address', 'Destination Port', and 'Destination Transport Type'. ▪ **[2]** Request URI = The INVITE is sent to the address indicated in the incoming Request-URI. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these fields take precedence. ▪ **[3]** ENUM = An ENUM query is sent to include the destination address. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request URI parameters are overridden and these fields take precedence.
Destination IP Group ID **[IP2IPRouting_DestIPGroupID]**	The IP Group ID to where you want to route the call. The INVITE messages are sent to the IP address(es) 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, the IP Group takes precedence. If the destination IP Group is of USER type, 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. The default is -1. **Note:** 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

Parameter	Description
Destination Address **[IP2IPRouting_DestAddress]**	The destination IP address (or domain name, e.g., domain.com) to where the call is sent. **Notes:** ▪ This parameter is applicable only if the parameter 'Destination Type' is set to 'Dest Address' [1]. ▪ 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 88).
Destination Port **[IP2IPRouting_DestPort]**	The destination port to where the call is sent.
Destination Transport Type **[IP2IPRouting_DestTransportType]**	The transport layer type for sending the call: ▪ **[-1]** Not Configured (default) ▪ **[0]** UDP ▪ **[1]** TCP ▪ **[2]** TLS **Note:** When this parameter is set to -1, the transport type is determined by the parameter SIPTransportType.

3.4 Maintenance Tab

The **Maintenance** tab on the Navigation bar displays menus in the Navigation tree related to device maintenance procedures. These menus include the following:

- Maintenance (see "Maintenance" on page 166)
- Software Update (see "Software Update" on page 170)

3.4.1 Maintenance

The **Maintenance** menu allows you to perform various maintenance procedures. This menu contains the following page item:

- Maintenance Actions (see "Maintenance Actions" on page 166)

3.4.1.1 Maintenance Actions

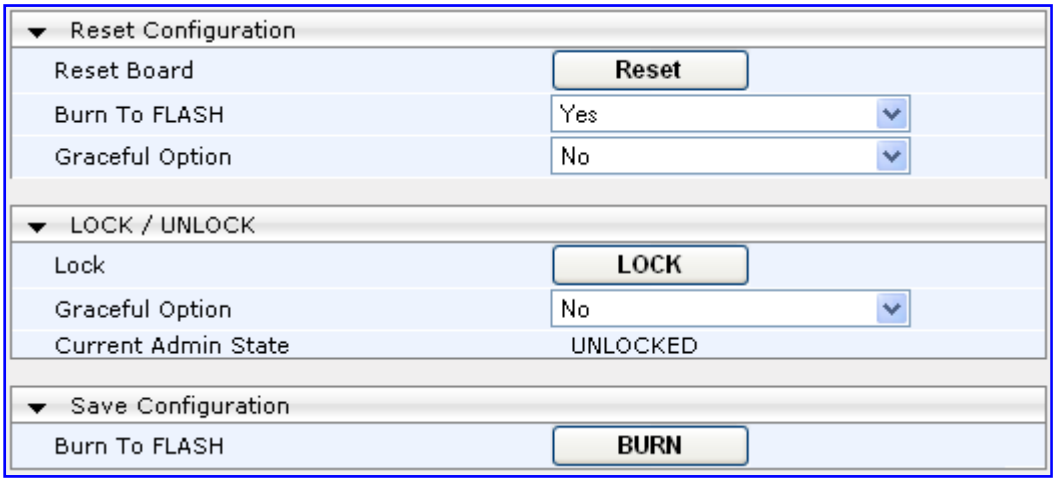
The 'Maintenance Actions' page allows you to perform the following:

- Reset the device (see "Resetting the Device" on page 167)
- Lock and unlock the device (see "Locking and Unlocking the Device" on page 168)
- Save configuration to the device's flash memory (see "Saving Configuration" on page 169)

➢ **To access the 'Maintenance Actions' page:**

- On the Navigation bar, click the **Maintenance** tab, and then in the Navigation tree, select the **Maintenance** menu, and then choose **Maintenance Actions**.

Figure 3-103: Maintenance Actions Page



3.4.1.1.1 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, i.e., device reset starts only after a user-defined time (i.e., timeout) or after no more active traffic exists (the earliest thereof).

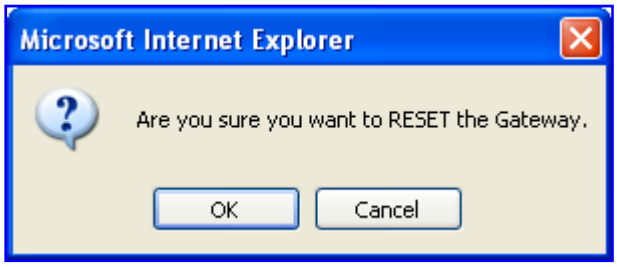
Notes:

- Throughout the Web interface, parameters preceded by the 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 the word "Reset" (see "Toolbar" on page 31) to indicate that a device reset is required.

➢ **To reset the device:**

1. Open the 'Maintenance Actions' page (see "Maintenance Actions" on page 166).
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 3-104: 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.

3.4.1.1.2 Locking and Unlocking the Device

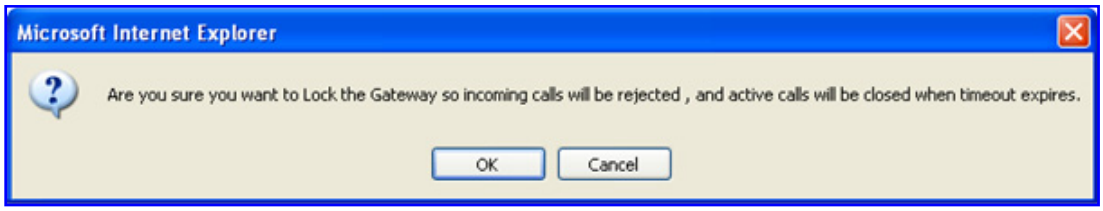
The Lock and Unlock options allow you to lock the device so that it doesn't accept any new calls. This is useful when, for example, you are uploading new software files to the device and you don't want any traffic to interfere with the process.

➢ **To lock the device:**

1. Open the 'Maintenance Actions' page (see "Maintenance Actions" on page 166).
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 3-105: 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 166).
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 "Using the Home Page" on page 53).

3.4.1.1.3 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 "Maintenance Actions" on page 166).
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 168).
- Throughout the Web interface, parameters preceded by 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 167).
- The Home page's General Information pane displays whether the device is currently "burning" the configuration (see "Using the Home Page" on page 53).

3.4.2 Software Update

The **Software Update** menu allows you to upgrade the device's software, install Software Upgrade Key, and load/save configuration file. This menu includes the following page items:

- Load Auxiliary Files (see "Loading Auxiliary Files" on page 170)
- Software Upgrade Key (see "Loading Software Upgrade Key" on page 172)
- Software Upgrade Wizard (see "Software Upgrade Wizard" on page 175)
- Configuration File (see "Backing Up and Loading Configuration File" on page 178)

3.4.2.1 Loading Auxiliary Files

The 'Load Auxiliary Files' page allows you to load various auxiliary files to the device. These auxiliary files are briefly described in the table below:

Table 3-28: Auxiliary Files Descriptions

File	Description
INI	Provisions the device's parameters. The Web interface enables practically full device provisioning, but customers may occasionally require new feature configuration parameters in which case this file is loaded. **Note:** Loading this file only provisions those parameters that are included in the *ini* file. For a detailed description on the *ini* file, see "INI File-Based Management" on page 193.
Call Progress Tones	This is a 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 a detailed description of the CPT file, see "Call Progress Tones File" on page 217.
Prerecorded Tones	The Prerecorded Tones (PRT) file enhances the device's capabilities of playing a wide range of telephone exchange tones that cannot be defined in the CPT file. For a detailed description of the PRT file, see "Prerecorded Tones File" on page 222.
Dial Plan	This file contains dialing plans, used by the device, for example, to know when to stop collecting the dialed digits and start sending them on. For a detailed description of the Dial Plan file, see Dial Plan File on page 223.
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 a detailed description of the User Info file, see "User Information File" on page 224.

Notes:

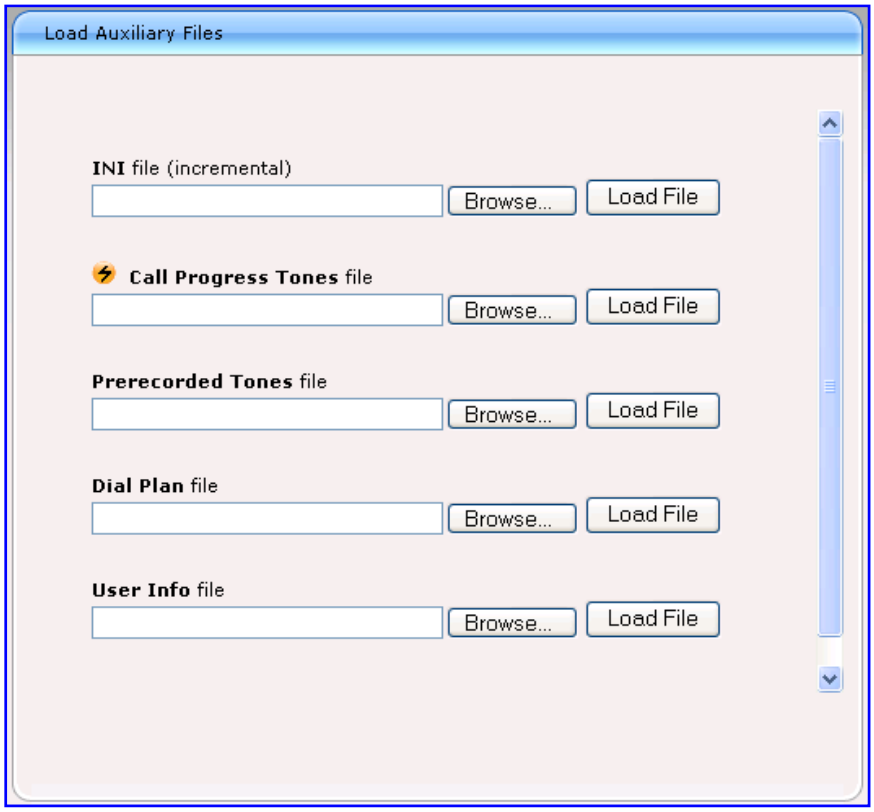
- You can schedule automatic loading of updated auxiliary files using HTTP/HTTPS, FTP, or NFS (for more details, refer to the *Product Reference Manual*).
- For a detailed description on auxiliary files, see "Auxiliary Configuration Files" on page 217.
- When loading an *ini* file using this Web page, 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 (see "Locking and Unlocking the Device" on page 168).
- For deleting auxiliary files, see "Viewing Device Information" on page 182.

The auxiliary files can be loaded to the device using the Web interface's 'Load Auxiliary Files' page, as described in the procedure below.

➢ **To load an auxiliary file to the device using the Web interface:**

1. Open the 'Load Auxiliary Files' page (**Maintenance** tab > **Software Update** menu > **Load Auxiliary Files**).

Figure 3-106: Load Auxiliary Files Page



Note: The appearance of certain file load fields depends on the installed Software Upgrade 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 169 and reset the device (if you have loaded a Call Progress Tones file), see "Resetting the Device" on page 167.

You can also load auxiliary files using an ini file that is loaded to the device with BootP. Each auxiliary file has a specific ini file parameter that specifies the name of the auxiliary file that you want to load to the device with the ini file. For a description of these ini file parameters, see Auxiliary and Configuration Files Parameters on page 496.

➢ **To load auxiliary files using an ini file:**

1. In the ini file, define the auxiliary files to be loaded to the device. You can also define in the ini file whether the loaded files must be stored in the non-volatile memory so that the TFTP process is not required every time the device boots up.
2. Save the auxiliary files and the ini file in the same directory on your local PC.
3. Invoke a BootP/TFTP session; the ini and associated auxiliary files are loaded to the device.

3.4.2.2 Loading Software Upgrade Key

The 'Software Upgrade Key Status' page allows you to load a new Software Upgrade Key to the device. The device is supplied with a Software Upgrade Key, which determines the device's supported features, capabilities, and available resources. The availability of certain Web pages depends on the loaded Software Upgrade Key. You can upgrade or change your device's supported features by purchasing a new Software Upgrade Key to match your requirements.

The Software Upgrade Key is provided in string format in a text-based file (*.out). When you load a Software Upgrade Key, it is loaded to the device's non-volatile flash memory and overwrites the previously installed key.

You can load a Software Upgrade Key using one of the following management tools:

- Web interface
- BootP/TFTP configuration utility (see Loading via BootP/TFTP on page 175)
- AudioCodes' EMS (refer to *EMS User's Manual* or *EMS Product Description*)

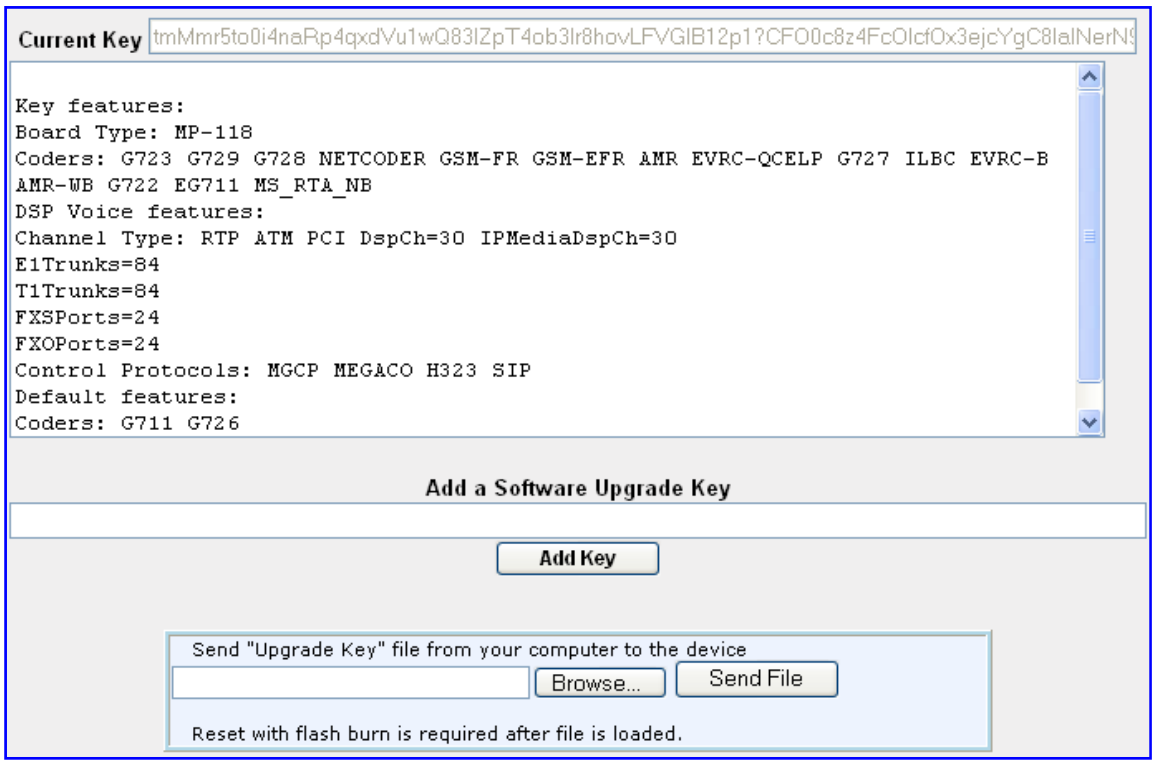
Warning: Do not modify the contents of the Software Upgrade Key file.

Note: The Software Upgrade Key is an encrypted key.

➢ **To load a Software Upgrade Key:**

1. Open the 'Software Upgrade Key Status' page (**Maintenance** tab > **Software Update** menu > **Software Upgrade Key**).

Figure 3-107: Software Upgrade Key Status Page



2. Backup your current Software Upgrade Key as a precaution so that you can re-load this backup key to restore the device's original capabilities if the new key doesn't comply with your requirements:
   a. In the 'Current Key' field, copy the string of text and paste it into any standard text file.
   b. Save the text file to a folder on your PC with a name of your choosing and file extension *.out.
3. Open the new Software Upgrade Key file and ensure that the first line displays '[LicenseKeys]' and that it contains one or more lines in the following format: S/N<serial number> = <long Software Upgrade Key string>

   For example: S/N370604 = jCx6r5tovCIKaBBbhPtT53Yj...

   One S/N must match the serial number of your device. The device's serial number can be viewed in the 'Device Information' page (see "Viewing Device Information" on page 182).
4. Follow one of the following procedures, depending on whether you are loading a single or multiple key S/N lines:
   - **Single key S/N line:**
     a. Open the Software Upgrade Key text file (using, for example, Microsoft® Notepad).
     b. Select and copy the key string and paste it into the field 'Add a Software Upgrade Key'.
     c. Click the **Add Key** button.

- **Multiple S/N lines (as shown below):**

Figure 3-108: Software Upgrade Key with Multiple S/N Lines

a. In the 'Send Upgrade Key file' field, click the **Browse** button and navigate to the folder in which the Software Upgrade Key text file is located on your PC.

b. Click the **Send File** button; the new key is loaded to the device and validated. If the key is valid, it is burned to memory and displayed in the 'Current Key' field.

5. Verify that the Software Upgrade Key file was successfully loaded to the device, by using one of the following methods:
   - In the 'Key features' group, ensure that the features and capabilities activated by the installed string match those that were ordered.
   - Access the Syslog server (refer to the *Product Reference Manual*) 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".
6. Reset the device; the new capabilities and resources are active.

Note: If the Syslog server indicates that the Software Upgrade Key file was unsuccessfully loaded (i.e., the 'SN_' line is blank), do the following preliminary troubleshooting procedures:

1. Open the Software Upgrade Key file and check that the S/N line appears. If it does not appear, contact AudioCodes.
2. Verify that you've loaded the correct file. Open the file and ensure that the first line displays [LicenseKeys].
3. Verify that the contents of the file have not been altered in any way.

3.4.2.2.1 Loading via BootP/TFTP

The procedure below describes how to load a Software Upgrade Key to the device using AudioCodes' BootP/TFTP Server utility (for a detailed description on the BootP utility, refer to the *Product Reference Manual*).

➢ **To load a Software Upgrade Key file using BootP/TFTP:**

1. Place the Software Upgrade Key file (typically, a *.txt file) in the same folder in which the device's *cmp* file is located.
2. Start the BootP/TFTP Server utility.
3. From the **Services** menu, choose **Clients**; the 'Client Configuration' screen is displayed.
4. From the 'INI File' drop-down list, select the Software Upgrade Key file. Note that the device's *cmp* file must be specified in the 'Boot File' field.
5. Configure the initial BootP/TFTP parameters as required, and then click **OK**.
6. Reset the device; the *cmp* and Software Upgrade Key files are loaded to the device.

Note: To load the Software Upgrade Key using BootP/TFTP, the extension name of the key file must be *.*ini*.

3.4.2.3 Software Upgrade Wizard

The Software Upgrade Wizard allows you to upgrade the device's firmware (compressed *cmp* file) as well as load an *ini* file and/or auxiliary files (typically loaded using the 'Load Auxiliary File' page described in "Loading Auxiliary Files" on page 170). 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 Saving and Resetting the Device).

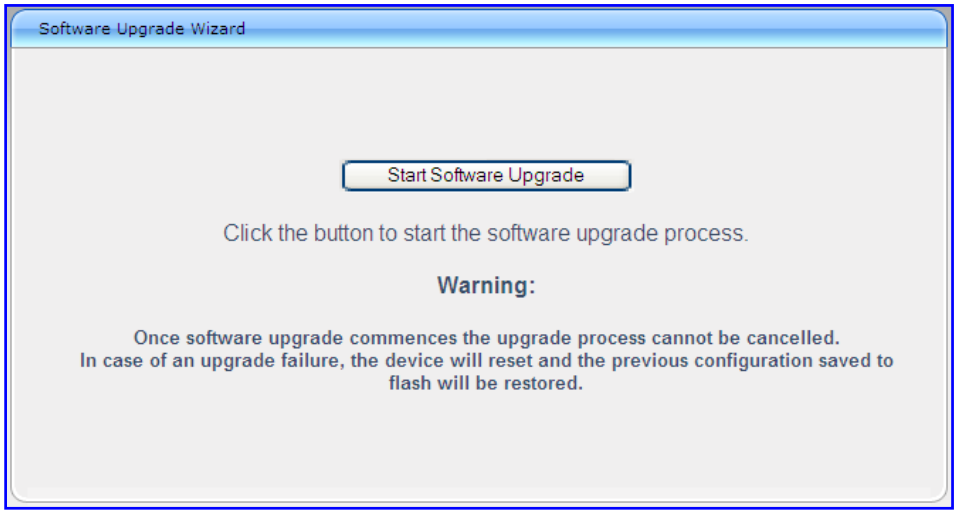
Notes:

- Before upgrading the device, it is recommended that you save a copy of the device's configuration settings (i.e., *ini* file) to your PC. 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 178.
- Before you can load an *ini* or auxiliary file, you must 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 Upgrade Key does not support the new cmp version. 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, FTP, or NFS (refer to the *Product Reference Manual*).

➢ 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' (**Maintenance** tab > **Software Update** menu > **Software Upgrade Wizard**); the 'Software Upgrade Wizard' page appears.

Figure 3-109: Start Software Upgrade Wizard Screen



3. Click the **Start Software Upgrade** button; the 'Load a CMP file' Wizard page appears.

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 **Send 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 Step 7.

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.

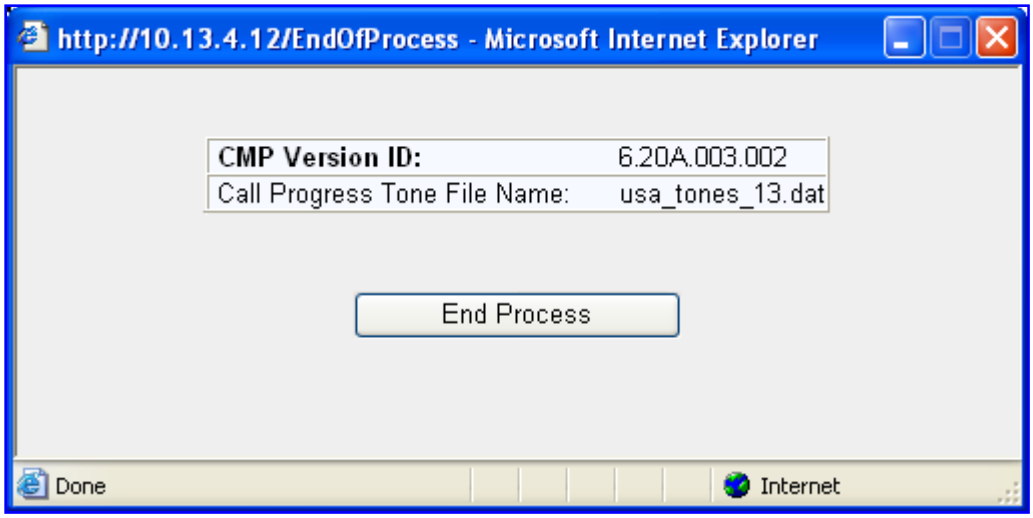
8. When you have completed loading all the desired files, click the **Next** button until the last wizard page appears ("FINISH" is highlighted in the left pane).

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 Process' screen appears displaying the burned configuration files:

Figure 3-110: End Process Wizard Page



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.

3.4.2.4 Backing Up and Loading Configuration File

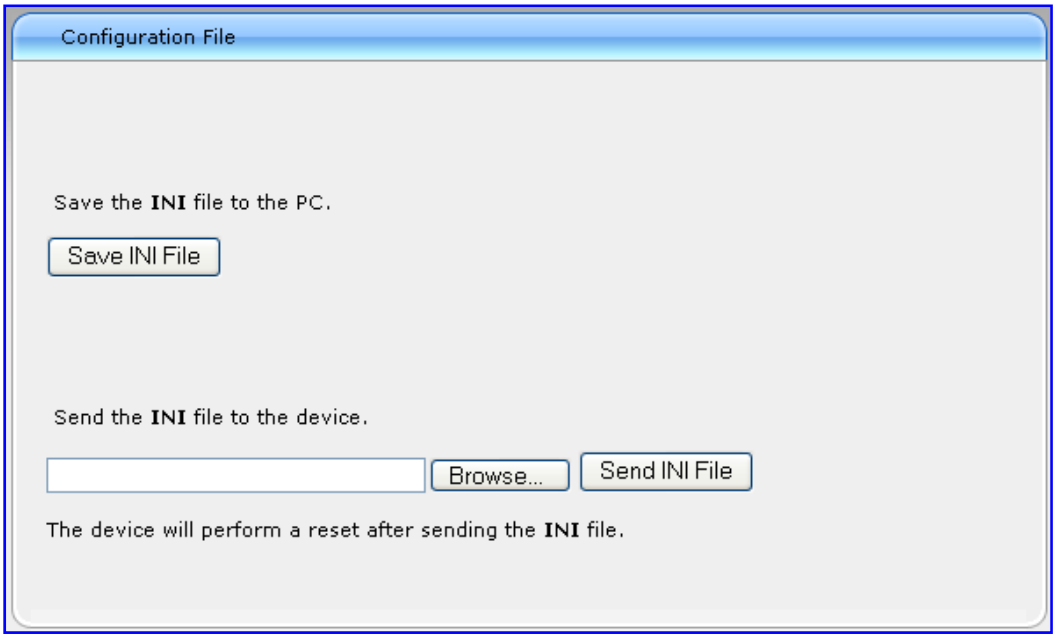
You can save a copy/backup of the device's current configuration settings as an *ini* file to a folder on your PC, using the 'Configuration File' page. The saved *ini* file includes only parameters that were modified and parameters with other than default values. The 'Configuration File' page also allows you to load an *ini* file to the device. If the device has "lost" its configuration, you can restore the device's configuration by loading the previously saved *ini* file or by simply loading a newly created *ini* file.

Note: When loading an *ini* file using this Web page, parameters not included in the *ini* file are reset to default settings.

➢ **To save / load the ini file:**

1. Open the 'Configuration File' page (**Maintenance** tab > **Software Update** menu > **Configuration File**). You can also access this page from the toolbar, by clicking **Device Actions**, and then choosing **Load Configuration File** or **Save Configuration File**.

Figure 3-111: Configuration File Page



2. To save the *ini* file to a folder on your PC, perform the following:
   a. Click the **Save INI File** button; the 'File Download' dialog box appears.
   b. Click the **Save** button, navigate to the folder in which you want to save the *ini* file on your PC, and then click **Save**; the device copies the *ini* file to the selected folder.
3. To load the *ini* file to the device, perform the following:
   a. Click the **Browse** button, navigate to the folder in which 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.
   a. Click the **Send 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 Login screen appears, requesting you to enter your user name and password.

3.5 Status & Diagnostics Tab

The **Status & Diagnostics** tab on the Navigation bar displays menus in the Navigation tree related to device operating status and diagnostics. These menus include the following:

- System Status (see "System Status" on page 180)
- VoIP Status (see "VoIP Status" on page 184)

3.5.1 System Status

The **System Status** menu is used to view and monitor the device's channels, Syslog messages, hardware and software product information, and to assess the device's statistics and IP connectivity information. This menu includes the following page items:

- Message Log (see Viewing Syslog Messages on page 180)
- Device Information (see "Viewing Device Information" on page 182)
- Ethernet Port Information (see "Viewing Ethernet Port Information" on page 182)
- Active Alarms (see "Viewing Active Alarms" on page 183)

3.5.1.1 Viewing Syslog Messages

The 'Message Log' page displays Syslog debug messages sent by the device. You can select the Syslog messages in this page, and then 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.

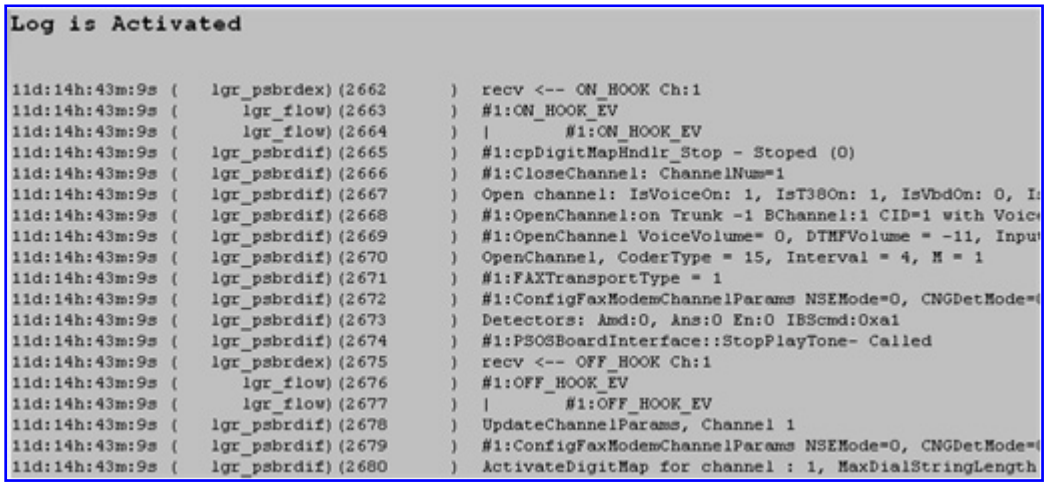
Notes:

- To enable Syslog functionality, use the EnableSyslog parameter (see "Configuring Syslog Settings" on page 61).
- 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 (refer to the *Product Reference Manual*).

➢ **To activate the Message Log:**

1. Activate and configure the device's Syslog client.
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 3-112: Message Log Page



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

3. To clear the page of Syslog messages, access the 'Message Log' page again (see Step 2); the page is cleared and new messages begin appearing.

➢ **To stop the Message Log:**

■ Close the 'Message Log' page by accessing any another page in the Web interface.

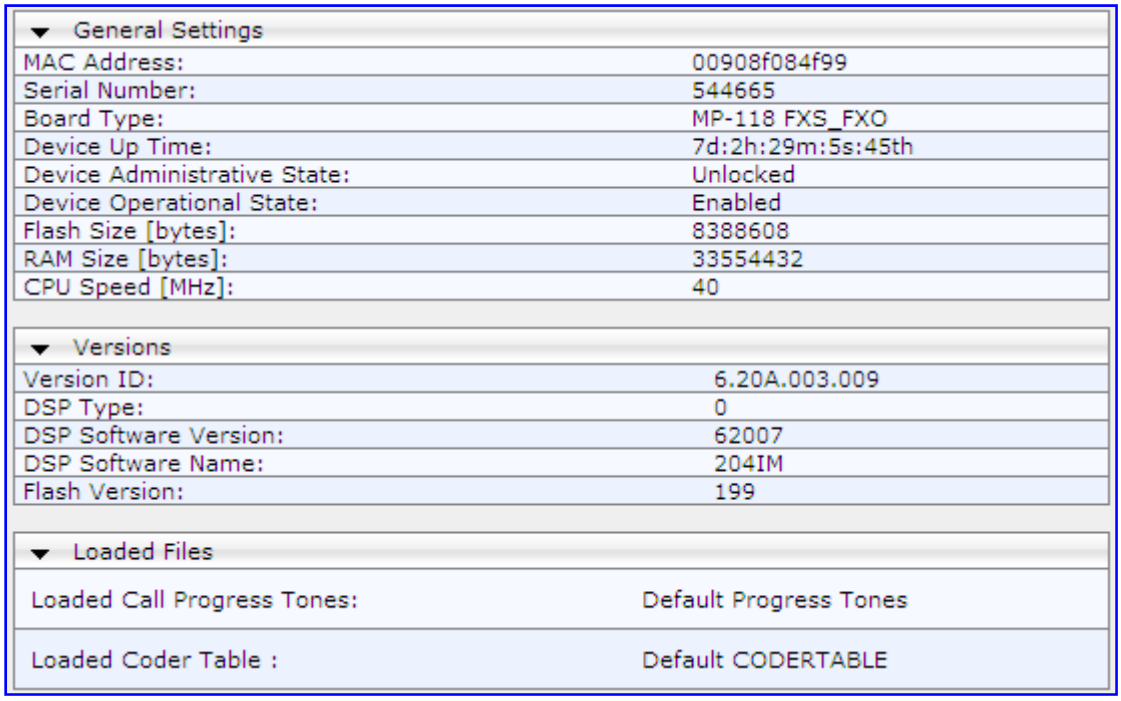
3.5.1.2 Viewing Device Information

The 'Device Information' page displays the device's specific hardware and software product information. This information can help you expedite troubleshooting. Capture the page and e-mail it to AudioCodes Technical Support personnel to ensure quick diagnosis and effective corrective action. This page also displays any loaded files used by the device (stored in the RAM) 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**).

Figure 3-113: Device Information Page



➢ **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 167).

3.5.1.3 Viewing Ethernet Port Information

The 'Ethernet Port Information' page displays read-only information on the device's Ethernet connection. This includes duplex mode, and speed. You can also access this page from the 'Home' page (see "Using the Home Page" on page 53).

For detailed information on the Ethernet redundancy scheme, see Ethernet Interface Redundancy. For detailed information on the Ethernet interface configuration, see "Ethernet Interface Configuration" on page 311.

➢ **To view Ethernet port information:**

- Open the 'Ethernet Port Information' page (**Status & Diagnostics** tab > **System Status** menu > **Ethernet Port Information**).

Figure 3-114: Ethernet Port Information Page

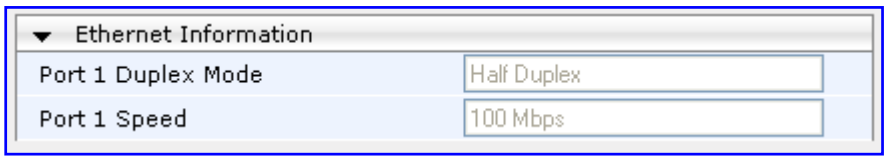


Table 3-29: Ethernet Port Information Parameters

Parameter	Description
Port Duplex Mode	Displays the Duplex mode of the Ethernet port.
Port Speed	Displays the speed (in Mbps) of the Ethernet port.

3.5.1.4 Carrier-Grade Alarms

The **Carrier-Grade Alarms** submenu contains the following item:

- Active Alarms (see "Viewing Active Alarms" on page 183)

3.5.1.4.1 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 "Using the Home Page" on page 53).

➢ **To view the list of alarms:**

- Open the 'Active Alarms' page (**Status & Diagnostics** tab > **System Status** menu > **Carrier-Grade Alarms** > **Active Alarms**).

For each alarm, the following information is provided:

- **Severity:** severity level of the alarm:
  - Critical - alarm displayed in red
  - Major - alarm displayed in orange
  - Minor - alarm displayed in 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 30 alarms (if exist), by pressing the F5 key.

3.5.2 VoIP Status

The **VoIP Status** menu allows you to monitor real-time activity of VoIP entities such as IP connectivity, call details, and call statistics. This menu includes the following page items:

- IP Interface Status (see "Viewing Active IP Interfaces" on page 184)
- Performance Statistics (see "Viewing Performance Statistics" on page 184)
- IP to Tel Calls Count (see "Viewing Call Counters" on page 185)
- Tel to IP Calls Count (see "Viewing Call Counters" on page 185)
- SAS Registered Users (see Viewing SAS/SBC Registered Users on page 187)
- Call Routing Status (see "Viewing Call Routing Status" on page 188)
- Registration Status (see Viewing Registration Status on page 189)
- IP Connectivity (see "Viewing IP Connectivity" on page 190)

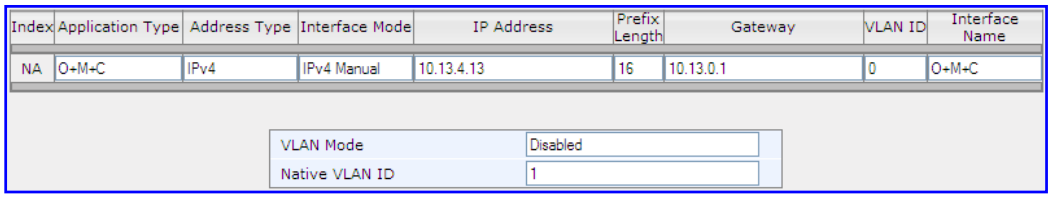
3.5.2.1 Viewing Active IP Interfaces

The 'IP Interface Status' page displays the device's active IP interfaces, which are configured in the 'Multiple Interface Table' page (see "Configuring IP Interface Settings" on page 78).

➢ **To view the 'Active IP Interfaces' page:**

- Open the 'IP Interface Status' page (**Status & Diagnostics** tab > **VoIP Status** menu > **IP Interface Status**).\

Figure 3-115: IP Interface Status Page



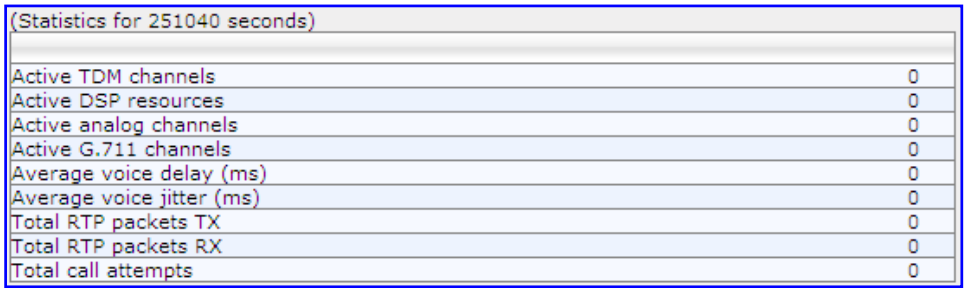
3.5.2.2 Viewing Performance Statistics

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 3-116: Basic Statistics Page



➢ **To reset the performance statistics to zero:**

- Click the **Reset Statistics** button.

3.5.2.3 Viewing Call Counters

The 'IP to Tel Calls Count' and 'Tel to IP Calls Count' pages 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 on the page.

➢ **To view the IP-to-Tel and Tel-to-IP Call Counters pages:**

- 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 3-117: 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

Table 3-30: Call Counters Description

Counter	Description
Number of Attempted Calls	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.
Number of Established Calls	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: ▪ GWAPP_REASON_NOT_RELEVANT (0) ▪ GWAPP_NORMAL_CALL_CLEAR (16) ▪ GWAPP_NORMAL_UNSPECIFIED (31) And the internal reasons: ▪ RELEASE_BECAUSE_UNKNOWN_REASON ▪ RELEASE_BECAUSE_REMOTE_CANCEL_CALL ▪ RELEASE_BECAUSE_MANUAL_DISC ▪ RELEASE_BECAUSE_SILENCE_DISC ▪ RELEASE_BECAUSE_DISCONNECT_CODE **Note:** When the duration of the call is zero, the release reason

Counter	Description
	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.
Percentage of Successful Calls (ASR)	The percentage of established calls from attempted calls.
Number of Calls Terminated due to a Busy Line	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)
Number of Calls Terminated due to No Answer	Indicates the number of calls that weren't answered. It's incremented as a result of one of the following release reasons: ▪ GWAPP_NO_USER_RESPONDING (18) ▪ GWAPP_NO_ANSWER_FROM_USER_ALERTED (19) ▪ GWAPP_NORMAL_CALL_CLEAR (16) (when the call duration is zero)
Number of Calls Terminated due to Forward	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
Number of Failed Calls due to No Route	Indicates the number of calls whose destinations weren't found. It is incremented as a result of one of the following release reasons: ▪ GWAPP_UNASSIGNED_NUMBER (1) ▪ GWAPP_NO_ROUTE_TO_DESTINATION (3)
Number of Failed Calls due to No Matched Capabilities	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.
Number of Failed Calls due to No Resources	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: ▪ GWAPP_RESOURCE_UNAVAILABLE_UNSPECIFIED ▪ RELEASE_BECAUSE_GW_LOCKED
Number of Failed Calls due to Other Failures	This counter is incremented as a result of calls that failed due to reasons not covered by the other counters.
Average Call Duration (ACD) [sec]	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.
Attempted Fax Calls Counter	Indicates the number of attempted fax calls.
Successful Fax Calls Counter	Indicates the number of successful fax calls.

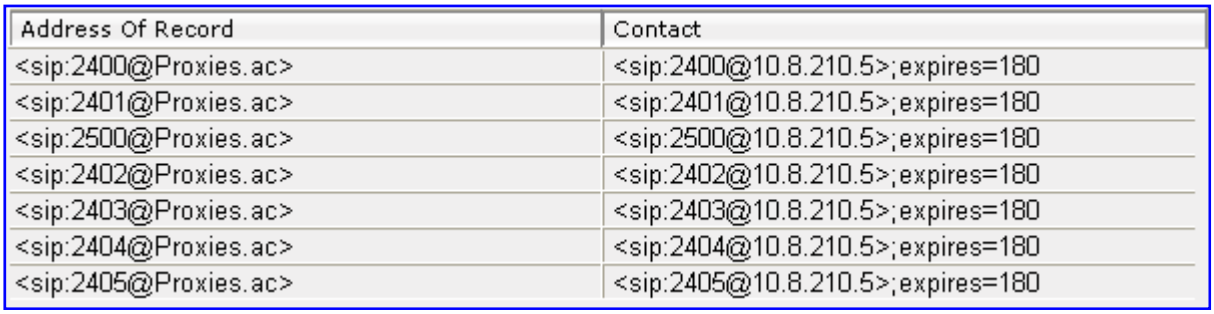
3.5.2.4 Viewing SAS/SBC Registered Users

The 'SAS/SBC Registered Users' page displays a list of registered SAS users recorded in the device's database.

➢ **To view the registered users:**

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

Figure 3-118: SAS/SBC Registered Users Page



Address Of Record	Contact
<sip:2400@Proxies.ac>	<sip:2400@10.8.210.5>;expires=180
<sip:2401@Proxies.ac>	<sip:2401@10.8.210.5>;expires=180
<sip:2500@Proxies.ac>	<sip:2500@10.8.210.5>;expires=180
<sip:2402@Proxies.ac>	<sip:2402@10.8.210.5>;expires=180
<sip:2403@Proxies.ac>	<sip:2403@10.8.210.5>;expires=180
<sip:2404@Proxies.ac>	<sip:2404@10.8.210.5>;expires=180
<sip:2405@Proxies.ac>	<sip:2405@10.8.210.5>;expires=180

Table 3-31: SAS/SBC Registered Users Parameters

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

3.5.2.5 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 the call routing status:**

- Open the 'Call Routing Status' page (**Status & Diagnostics** tab > **VoIP Status** menu > **Call Routing Status**).

Figure 3-119: Call Routing Status Page

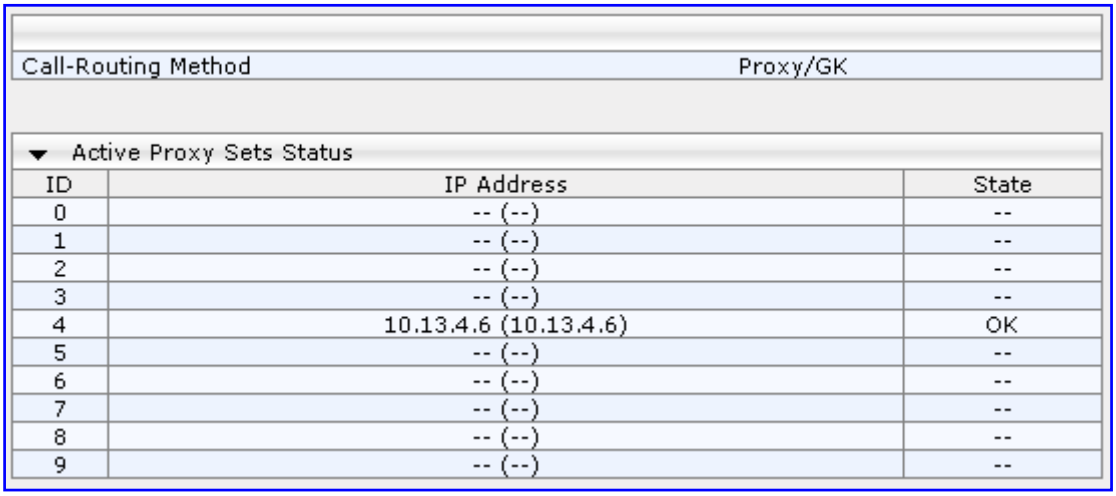


Table 3-32: Call Routing Status Parameters

Parameter	Description
Call-Routing Method	▪ Proxy/GK = Proxy server is used to route calls. ▪ Routing Table = The 'Tel to IP Routing' is used to route calls.
IP Address	▪ Not Used = Proxy server isn't defined. ▪ IP address and FQDN (if exists) of the Proxy server with which the device currently operates.
State	▪ N/A = Proxy server isn't defined. ▪ OK = Communication with the Proxy server is in order. ▪ Fail = No response from any of the defined Proxies.

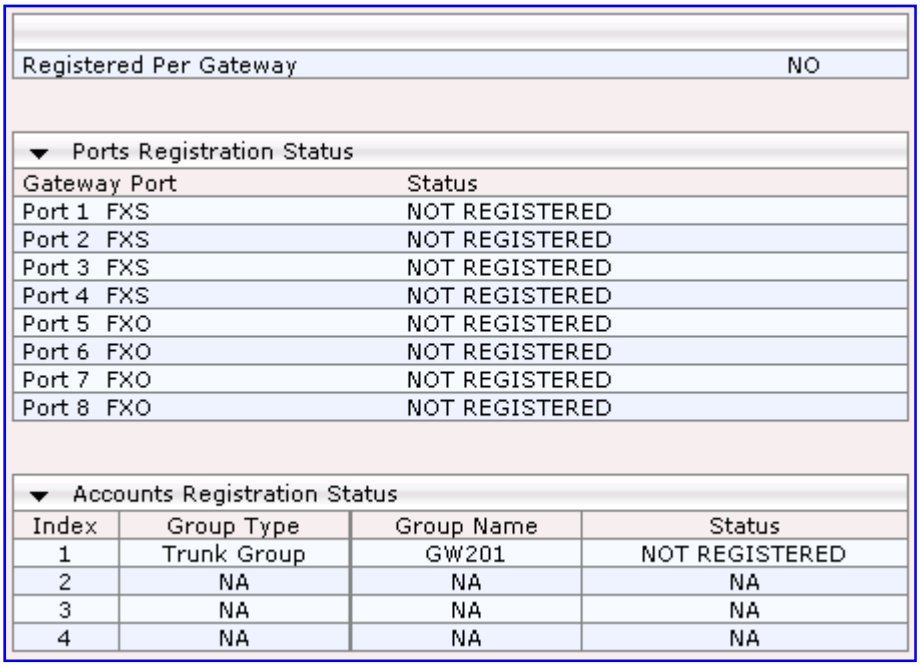
3.5.2.6 Viewing Registration Status

The 'Registration Status' page displays whether the device, its endpoints, SIP Accounts, and BRI endpoints are registered to a SIP Registrar/Proxy server.

➢ **To view Registration status:**

- Open the 'Registration Status' page (**Status & Diagnostics** tab > **VoIP Status** menu > **Registration Status**).

Figure 3-120: Registration Status Page



Registered Per Gateway NO

Ports Registration Status

Gateway Port	Status
Port 1 FXS	NOT REGISTERED
Port 2 FXS	NOT REGISTERED
Port 3 FXS	NOT REGISTERED
Port 4 FXS	NOT REGISTERED
Port 5 FXO	NOT REGISTERED
Port 6 FXO	NOT REGISTERED
Port 7 FXO	NOT REGISTERED
Port 8 FXO	NOT REGISTERED

Accounts Registration Status

Index	Group Type	Group Name	Status
1	Trunk Group	GW201	NOT REGISTERED
2	NA	NA	NA
3	NA	NA	NA
4	NA	NA	NA

- **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 113):
  - **Group Type:** type of served group - Hunt 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')

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 126) or using the TrunkGroupSettings *ini* file parameter.

3.5.2.7 Viewing IP Connectivity

The 'IP Connectivity' page displays online, read-only network diagnostic connectivity information on all destination IP addresses configured in the 'Tel to IP Routing' page (see "Configuring Tel to IP Routing" on page 138).

Notes:

- This information is available only if the parameter 'Enable Alt Routing Tel to IP'/AltRoutingTel2IPMode (see "Configuring General Routing Parameters" on page 137) is set to 1 (Enable) or 2 (Status Only).
- 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 parameter 'Enable Alt Routing Tel to IP' (or *ini* file parameter AltRoutingTel2IPEnable) to Enable **[1]** or Status Only **[2]**.
2. Open the 'IP Connectivity' page (**Status & Diagnostics** tab > **VoIP Status** menu > **IP Connectivity**).

Figure 3-121: IP Connectivity Page

	IP Address	Host Name	Connectivity Method	Connectivity Status	Quality Status	Quality Info	DNS Status
1	Unused	---	---	---	---	---	---
2	Unused	---	---	---	---	---	---
3	Unused	---	---	---	---	---	---
4	Unused	---	---	---	---	---	---
5	Unused	---	---	---	---	---	---
6	Unused	---	---	---	---	---	---
7	Unused	---	---	---	---	---	---
8	Unused	---	---	---	---	---	---
9	Unused	---	---	---	---	---	---
10	Unused	---	---	---	---	---	---

Table 3-33: IP Connectivity Parameters

Column Name	Description
IP Address	The IP address can be one of the following: ▪ IP address defined as the destination IP address in the 'Tel to IP Routing'. ▪ IP address resolved from the host name defined as the destination IP address in the 'Tel to IP Routing'.
Host Name	Host name (or IP address) as defined in the 'Tel to IP Routing'.
Connectivity Method	The method according to which the destination IP address is queried periodically (ICMP ping or SIP OPTIONS request).
Connectivity Status	The status of the IP address' connectivity according to the method in the 'Connectivity Method' field. ▪ OK = Remote side responds to periodic connectivity queries. ▪ Lost = Remote side didn't respond for a short period. ▪ Fail = Remote side doesn't respond. ▪ Init = Connectivity queries not started (e.g., IP address not resolved). ▪ Disable = The connectivity option is disabled, i.e., parameter 'Alt Routing Tel to IP Mode' (AltRoutingTel2IPMode *ini*) is set to 'None' or 'QoS'.

Column Name	Description
Quality Status	Determines the QoS (according to packet loss and delay) of the IP address. ▪ Unknown = Recent quality information isn't available. ▪ OK ▪ Poor **Notes:** ▪ This parameter is applicable only if the parameter 'Alt Routing Tel to IP Mode' is set to 'QoS' or 'Both' (AltRoutingTel2IPMode = 2 or 3). ▪ This parameter is reset if no QoS information is received for 2 minutes.
Quality Info.	Displays QoS information: delay and packet loss, calculated according to previous calls. **Notes:** ▪ This parameter is applicable only if the parameter 'Alt Routing Tel to IP Mode' is set to 'QoS' or 'Both' (AltRoutingTel2IPMode = 2 or 3). ▪ This parameter is reset if no QoS information is received for 2 minutes.
DNS Status	DNS status can be one of the following: ▪ DNS Disable ▪ DNS Resolved ▪ DNS Unresolved

Reader's Notes

4 INI File-Based Management

The device can also be configured by loading an *ini* file, which contains user-defined parameters. The *ini* file can be loaded to the device using the following methods:

- Web interface (see "Backing Up and Loading Configuration File" on page 178)
- AudioCodes' BootP/TFTP utility (refer to the Product Reference Manual)
- Any standard TFTP server

The *ini* file configuration parameters are saved in the device's non-volatile memory when the file is loaded to the device. If a parameter is excluded from the loaded *ini* file, the following occurs depending on how you load the file:

- 'Load Auxiliary Files' page (see "Loading Auxiliary Files" on page 170): current settings are retained for excluded parameters
- All other methods: default value is assigned to excluded parameters (according to the *cmp* file running on the device), thereby, overriding values previously defined for these parameters

Notes:

- For a list and description of the *ini* file parameters, see "Configuration Parameters Reference" on page 333.
- 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 Default Settings" on page 215.

4.1 INI File Format

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

- Individual parameters (see "Configuring Individual ini File Parameters" on page 193)
- Table parameters (see "Configuring ini File Table Parameters" on page 194)

4.1.1 Configuring Individual ini File Parameters

The format of individual *ini* file parameters includes an optional, subsection name (group name) to conveniently group similar parameters by their functionality. Following this line are the actual parameter settings. These format lines are shown below:

```
[subsection name]
; the subsection name is optional.
Parameter Name = Parameter Value
Parameter Name = Parameter Value
; Remark
```

For general *ini* file formatting rules, see "General ini File Formatting Rules" on page 196.

An example of an *ini* file containing individual *ini* file parameters is shown below:

```
[System Parameters]
SyslogServerIP = 10.13.2.69
EnableSyslog = 1
; these are a few of the system-related parameters.
[Web Parameters]
LogoWidth = '339'
WebLogoText = 'My Device'
UseWeblogo = 1
; these are a few of the Web-related parameters.
[Files]
CallProgressTonesFileName = 'cpusa.dat'
```

4.1.2 Configuring ini File Table Parameters

The *ini* file table parameters allow you to configure tables which can 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 *ini* file table 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 an *ini* file table 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 *ini* file table 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 196.

The table below displays an example of an *ini* file table 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 2 = eg711Ulaw, 10, 0, 71, 0;
[ \CodersGroup0 ]
```

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

4.1.3 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.

4.2 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 current *ini* file from the device to your PC, using the Web interface (see "Backing Up and Loading Configuration File" on page 178).
2. Open the *ini* file (using a text file editor such as Microsoft Notepad), and then modify the *ini* file parameters according to your requirements.
3. Save the modified *ini* file, and then close the file.
4. Load the modified *ini* file to the device, using the BootP/TFTP utility or the Web interface (see "Backing Up and Loading Configuration File" on page 178).

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

4.3 Secured Encoded ini File

The *ini* file contains sensitive information that is required for the functioning of the device. Typically, it is loaded to or retrieved from the device using TFTP or HTTP. These protocols are not secure and are vulnerable to potential hackers. To overcome this security threat, the AudioCodes' TrunkPack Downloadable Conversion Utility (DConvert) utility allows you to binary-encode (encrypt) the *ini* file before loading it to the device (refer to the *Product Reference Manual)*.

Notes:

- The procedure for loading an encoded *ini* file is identical to the procedure for loading an unencoded *ini* file (see Backing Up and Restoring Configuration).
- If you download from the device (to a folder on your PC) an *ini* file that was loaded encoded to the device, the file is saved as a regular *ini* file (i.e., unencoded).

Reader's Notes

5 EMS-Based Management

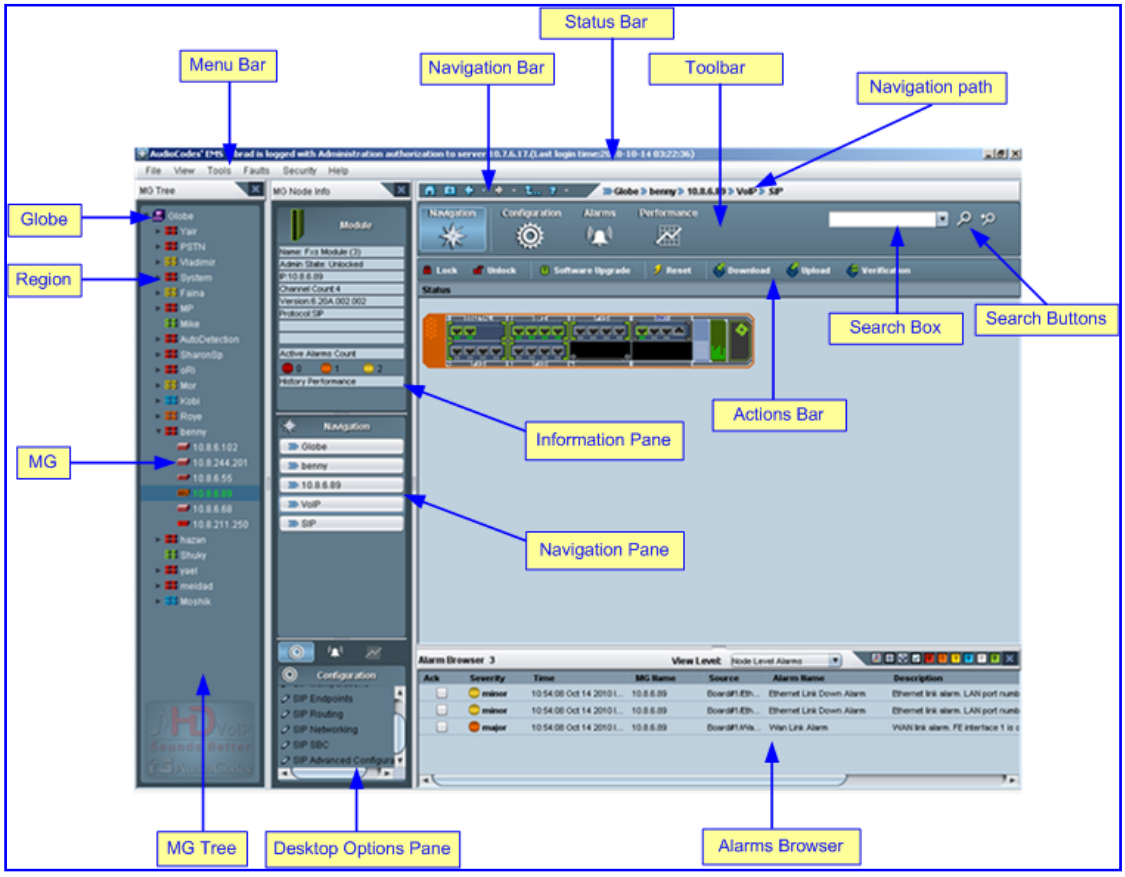
This section provides a brief description on configuring various device configurations using AudioCodes Element Management System (EMS). The EMS is an advanced solution for standards-based management of gateways within VoP networks, covering all areas vital for the efficient operation, administration, management and provisioning (OAM&P) of AudioCodes' families of gateways. 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 a detailed description of using the EMS tool, refer to the *EMS User's Manual* and *EMS Server IOM Manual*.

5.1 Familiarizing yourself with EMS GUI

The areas of the EMS graphical user interface (GUI) are shown in the figure below:

Figure 5-1: Areas of the EMS GUI



The MG Tree is a hierarchical tree-like structure that lists all the devices managed by EMS. The tree includes the following icons:

- **Globe** : highest level in the tree from which a Region can be added.
- **Region** : defines a group (e.g., geographical location) to which devices can be added. If you click a Region that is defined with devices (MG's), the Main pane (see figure above) displays a list of all the devices pertaining to the Region.
- **MG** : defines the device. This is the lowest level in the tree. If you click an **MG** icon, the Main pane (see figure above) displays a graphical representation of the device's chassis.

5.2 Securing EMS-Device Communication

5.2.1 Configuring IPSec

Before you can configure the device through the EMS, you need to configure the secure communication protocol IPSec for communicating between the EMS and the device. Before you enable IPSec in the EMS, you must define the IPSec IKE pre-shared key in a secure manner. This is performed through an SSH secure shell client session (e.g. PuTTY). Once you have defined the IPSec IKE pre-shared key, you must enter the same IPSec IKE pre-shared key in the EMS when you define the device.

Before performing the procedure below, ensure that you have the following information:

- The IP address of the EMS Server that is to communicate with the device
- An initial password for the IKE pre-shared key

Notes:

- The device is shipped with SSH enabled.
- The configuration text is case- and space-sensitive. Type the text rather than copy-and-paste. Save the IKE pre-shared key as later on you need to enter the same value in the EMS when defining the device.
- For more information on CLI, refer to the *Product Reference Manual.*
- For more information on securing communication protocols, refer to the *EMS Users Manual*.

➢ **To configure the device for communicating via IPSec with the EMS:**

1. Open an SSH Client session (e.g. PuTTY), and then connect to the device.
   - If a message appears with the RSA host key, click **Yes** to continue.
   - The default username and password are "Admin" (case-sensitive). Verify that the shell prompt appears ("\> ").
2. Type **Conf**, and then press Enter.
   ```
   /CONFiguration>
   ```
3. Type **cf set**, and then press Enter; the following prompt is displayed:
   ```
   Enter data below. Type a period (.) on an empty line to
   finish.
   ```
   The configuration session is now active and all data entered at the terminal is parsed as configuration text (formatted as an *ini* file).
4. Type the following at the configuration session:

```
[ IPsecSATable ]
FORMAT IPsecSATable Index =
IPsecSATable RemoteEndpointAddressOrName,
IPsecSATable_AuthenticationMethod, IPsecSATable_SharedKey,
IPsecSATable SourcePort, IPsecSATable DestPort,
IPsecSATable Protocol, IPsecSATable Phase1SaLifetimeInSec,
IPsecSATable_Phase2SaLifetimeInSec,
IPsecSATable Phase2SaLifetimeInKB, IPsecSATable DPDmode,
IPsecSATable IPsecMode, IPsecSATable RemoteTunnelAddress,
IPsecSATable RemoteSubnetIPAddress,
IPsecSATable RemoteSubnetPrefixLength, IPsecSATable InterfaceName;
IPsecSATable 1 = <IP address>, 0, <IKE password>, 0, 0, 0, 28800,
28800, 0, 0, 0, 0.0.0.0, 0.0.0.0, 16, ;
[ \IPsecSATable ]
EnableIPSec = 1
```

where:

- <IKE password> is the password for the initial IKE pre-shared key.
- <IP address> is the IP address of the EMS server used for connecting to the device for which IPSec connectivity is established.

5. To end the PuTTY configuration session, type a full-stop (".") on an empty line; the device responds with the following:

   ```
   INI File replaced
   ```

6. To save the configuration to the non-volatile memory, type **sar**; the device reboots with IPSec enabled.

Note: If you have enabled IPSec and you want to change the IP address and/or IKE password, you need to first disable IPSec. Perform the procedure as above, but omit the lines [IPsecSATable], and set EnableIPSec to 0. Once you have done this, repeat the exact procedure as described above, but with the new IP address and/or password.

5.2.2 Changing SSH Login Password

For security, it is recommended to change the default SSH Client login password, using the SSH client.

➢ **To change the SSH login password:**

1. Open an SSH Client session (e.g. PuTTY), and then connect, using the default user name and password ("Admin" - case sensitive), to the device. If a message appears with the RSA host key, click **Yes** to continue; the shell prompt appears ("\> ").
2. At the CLI prompt, type the command **chpw** and specify the existing and new passwords.

   ```
   chpw <old_password> <new_password>
   ```

   where:

   - <old_password> is the existing password
   - <new_password> is the new password

   The device responds with the message "Password changed".
3. Close the SSH client session and reconnect using the new password.

Note: The default user name ("Admin") cannot be changed from within an SSH client session.

5.3 Adding the Device in EMS

Once you have defined the IPSec communication protocol for communicating between EMS and the device and configured the device's IP address (refer to the *Installation Manual*), you can add the device in the EMS.

Adding the device to the EMS includes the following main stages:

a. Adding a Region

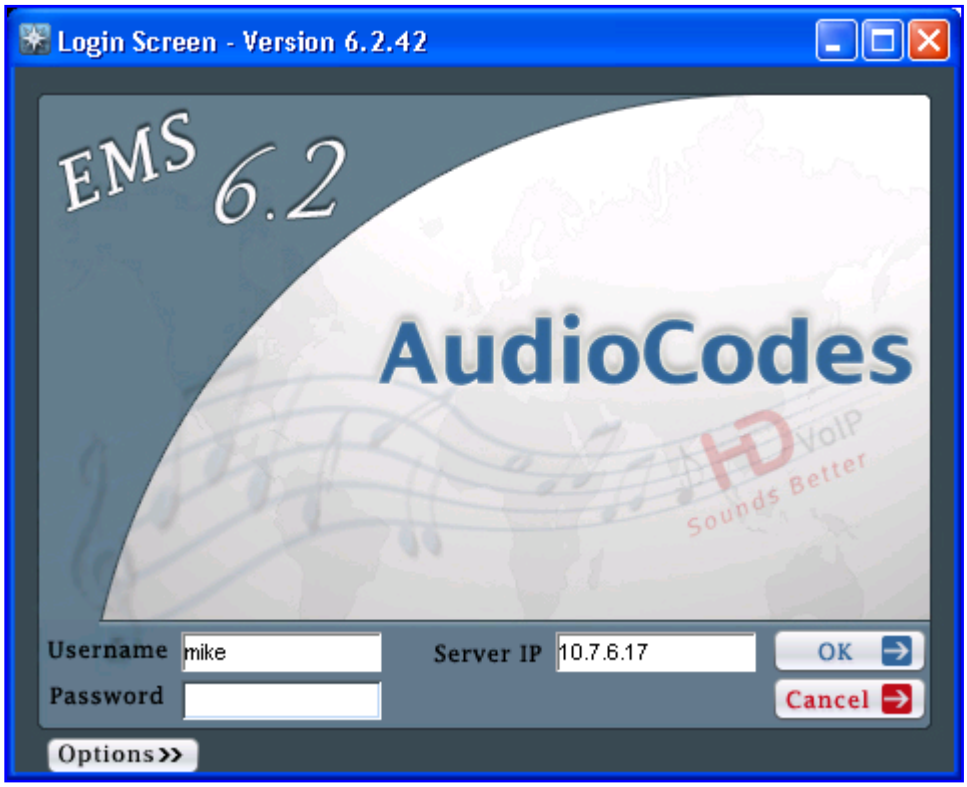
b. Defining the device's IP address (and other initial settings)

➢ **To initially setup the device in EMS:**

1. Start the EMS by double-clicking the shortcut icon

on your desktop, or from the **Start** menu, point to **Programs**, point to **EMS Client**, and then click **EMS Client**; the Login Screen appears:

Figure 5-2: EMS Login Screen



2. Enter your login username and password, the EMS server's IP address, and then click **OK**.

3. Add a Region for your deployed device, by performing the following:

a. In the MG Tree, right-click the **Globe** icon, and then click **Add Region**; the Region dialog box appears.

Figure 5-3: Adding a Region

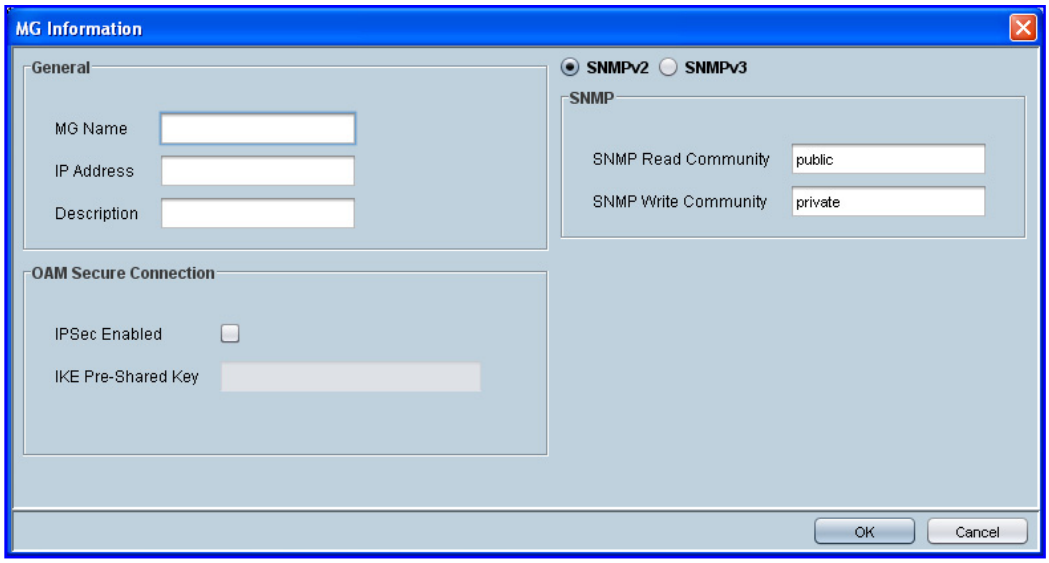
b. In the 'Region Name' field, enter a name for the Region (e.g., a geographical name), and then click **OK**; the Region is added to the MG Tree list.

4. Verify that the device is up and running (by performing a ping to its IP address).

5. Add the device to the Region, by performing the following:

a. Right-click the added Region icon, and then from the shortcut menu, choose **Add MG**; the MG Information dialog box appears.

Figure 5-4: Defining the IP Address



b. Enter an arbitrary name for the device, and then in the 'IP Address' field, enter the device's IP address

c. Ensure that 'IPSec Enabled' check box is selected, and then enter the IPSec Preshared Key (defined in Configuring IPSec on page 200).

d. Click **OK**; the device is added to the Region and appears listed in the MGs List.

Note: The Pre-shared Key string defined in the EMS must be identical to the one that you defined for the device. When IPSec is enabled, default IPSec/IKE parameters are loaded to the device.

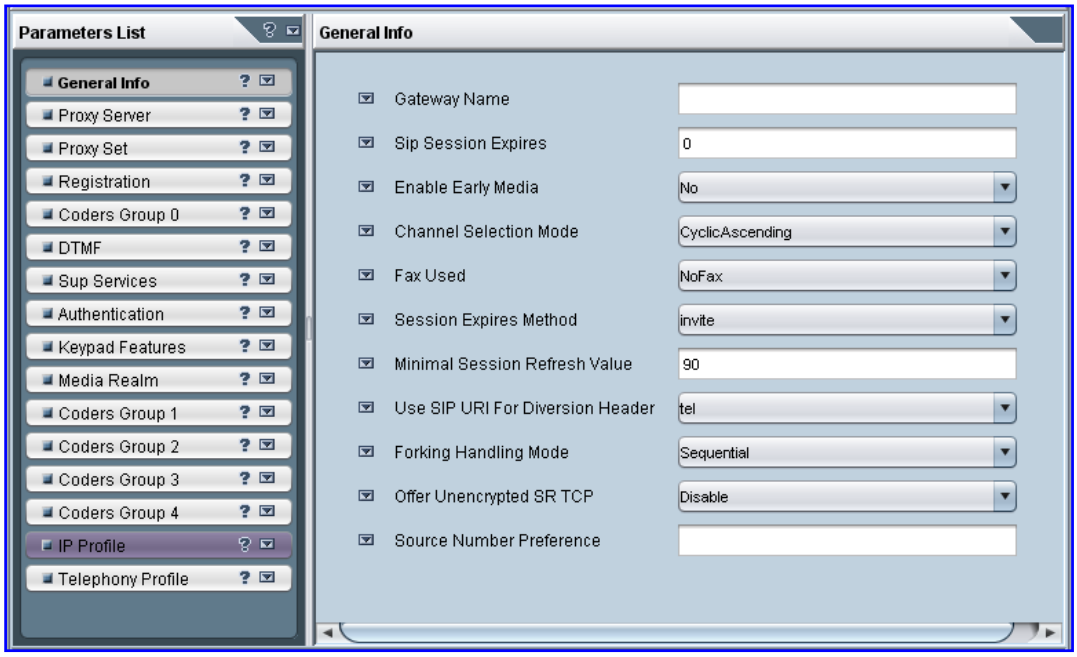
5.4 Configuring Basic SIP Parameters

This section describes how to configure the device with basic SIP control protocol parameters using the EMS.

➢ **To configure basic SIP parameters:**

1. In the **Navigation** pane, select **VoIP** > **SIP**, and then in the **Configuration** pane, select **SIP Protocol Definitions**; the 'SIP Protocol Definitions' frame appears.

Figure 5-5: SIP Protocol Definitions Frame



2. Select the **Coders Group 0** tab; the Coders screen is displayed.
   a. Click the button to add a new Coder entry, and then click **Yes** to confirm.
   b. Double-click each field to enter values.
   c. Right-click the new entry, and then choose **Unlock Rows**.
3. Select the **Proxy Server** tab.
   a. Set 'Proxy Used' to Yes.
   b. (Optional) In the 'Proxy Name' field, enter the Proxy's name. The Proxy name replaces the Proxy IP address in all SIP messages. This means that messages are still sent to the physical Proxy IP address, but the SIP URI contains the Proxy name instead. When no Proxy is used, the internal routing table is used to route the calls.
   c. Click the button, and then click **Yes** to confirm.
   d. Enter the IP address of the Proxy Server.
   e. Right-click the new entry, and then choose **Unlock Rows**.
4. Select the **Registration** tab.
   a. Configure 'Is Register Needed' field:
      - No = the device doesn't register to a Proxy/Registrar server (default).
      - Yes = the device registers to a Proxy/Registrar server at power up and every user-defined interval (‘Registration Time’ parameter).
   b. Click **Apply** and close the active window.
5. Open the 'SIP EndPoints' frame (**Configuration** pane > **SIP Endpoints** menu).
   a. Click the button to add a new entry, and then click **Yes** to confirm; the 'Phones' screen is displayed.

b. Double-click each field to enter values.
c. Right-click the new entry, and then select **Unlock Rows.**
d. Click **Apply** and close the active window.

6. If a Proxy Server is not implemented, map outgoing telephone calls to IP addresses. Open the 'SIP Routing' frame (**Configuration** pane > **SIP Routing** menu).
   a. Select the **Tel to IP** tab.
   b. Click the button to add a new entry, and then click **Yes** to confirm; the Tel to IP Routing table is displayed.
   c. Double-click each field to enter values.
   d. Right-click the new entry and select **Unlock Rows**.
   e. Click **Apply** and close the active window.

5.5 Configuring Advanced IPSec/IKE Parameters

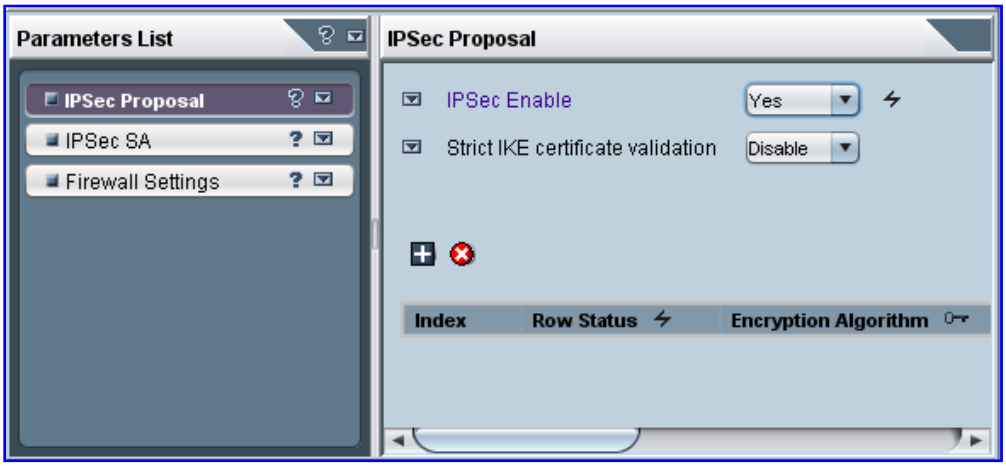
After you have pre-configured IPSec via SSH (see "Securing EMS-Device Communication" on page 200), you can optionally configure additional IPSec and IKE entries for other SNMP Managers aside from the EMS.

Note: Do not remove the default IPSec and IKE tables that were previously loaded to the device when you enabled IPSec.

➢ **To configure IPSec/IKE tables:**

1. In the **Navigation** pane, select **VoIP** > **Security**, and then in the **Configuration** pane, select **Security Frame**; the 'Security Provisioning' screen appears.
2. Select the **IPSec Proposal** tab; the 'IPSec Proposal' screen is displayed.

Figure 5-6: IPSec Table Screen



3. Select the button to add a new entry, and then click **Yes** at the confirmation prompt; a row is added to the table.
4. Enter the required values.
5. Right-click the new entry, and then from the shortcut menu, choose **Unlock rows**.
6. Click **Save**, and then **Close**.
7. Select the **IPSec SA** tab; the 'IPSec SA' screen appears.
8. Repeat steps 4 through 7.

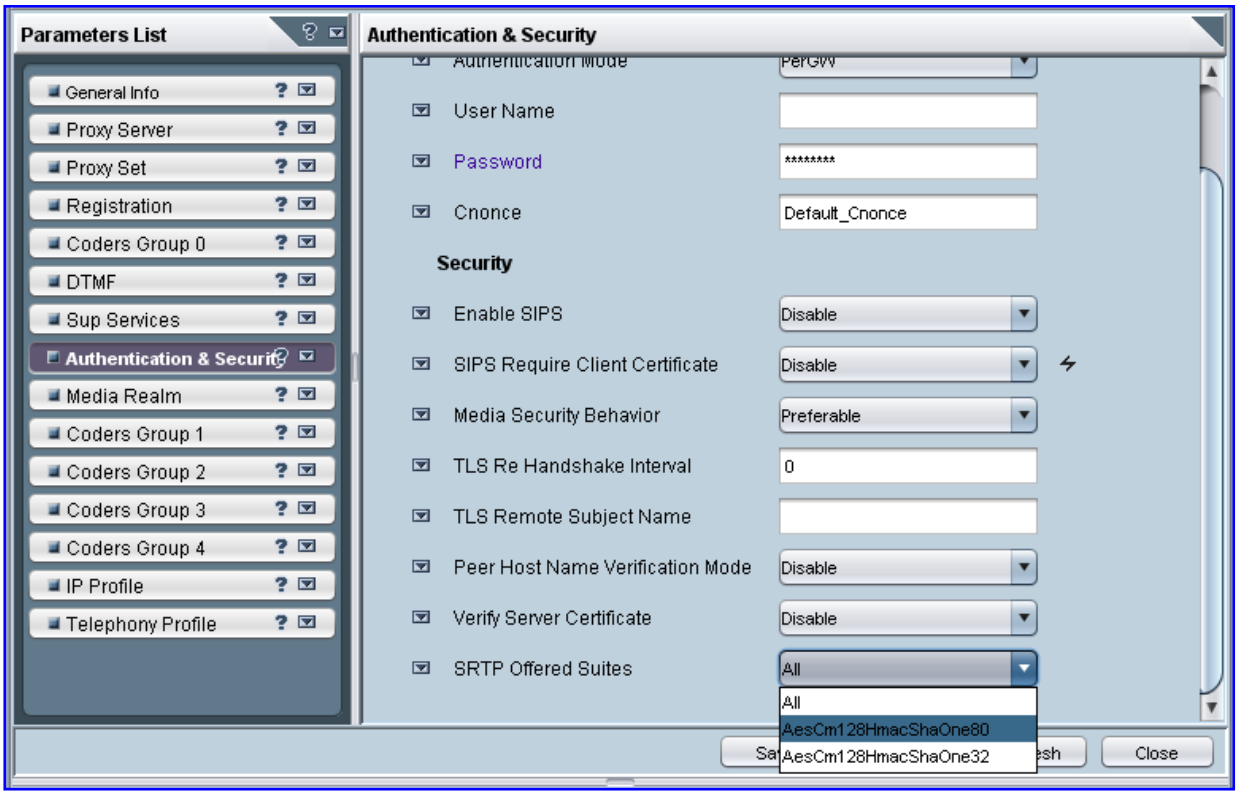
5.6 Provisioning SIP SRTP Crypto Offered Suites

This section describes how to configure offered SRTP crypto suites in the SDP.

➢ **To configure SRTP crypto offered suites:**

1. In the **Navigation** pane, select **VoIP** > **SIP**, and then in the **Configuration** pane, select **SIP Protocol Definitions**; 'SIP Protocol Definitions' frame appears.
2. Select the **Authentication & Security** tab; the 'Authentication & Security' screen appears.

Figure 5-7: Authentication & Security Screen



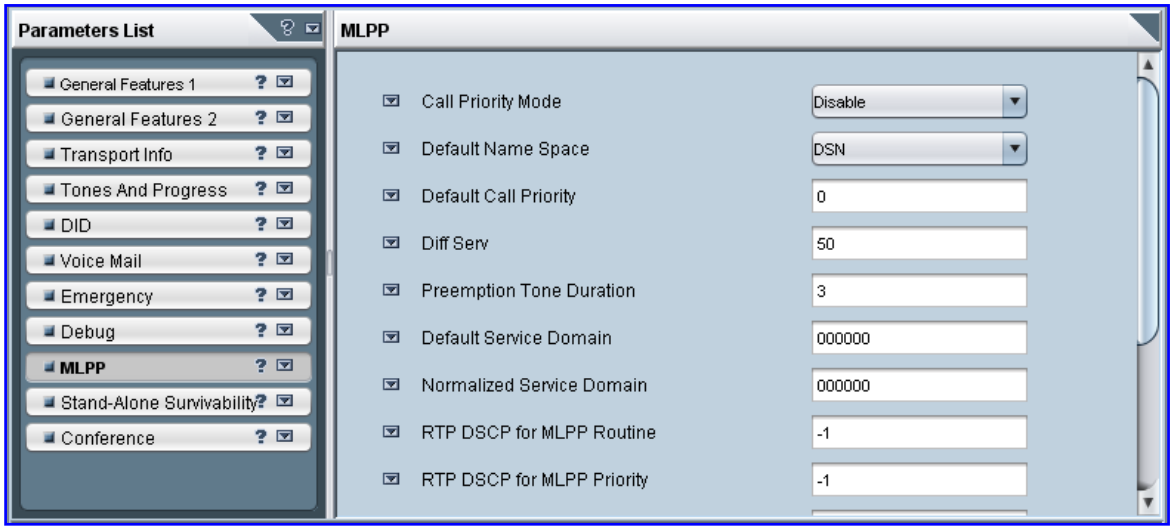
3. From the 'SRTP Offered Suites' (SRTPofferedSuites) drop-down list, select the required crypto suites.

5.7 Provisioning SIP MLPP Parameters

This section describes how to configure the MLPP (Multi-Level Precedence and Preemption) parameters using the EMS.

➢ **To configure the MLPP parameters:**

1. In the **Navigation** pane, select **VoIP** > **SIP**, and then in the **Configuration** pane, select **SIP Advanced Configuration**; 'SIP Advanced Configuration' frame appears.
2. Select the **MLPP** tab; the 'MLPP' screen appears.



3. Configure the MLPP parameters as required.

Note: If the following RTP DSCP parameters are set to "-1" (i.e., Not Configured, Default), the DiffServ value is set with the PremiumServiceClassMediaDiffserv global gateway parameter, or by using IP Profiles: MLPPRoutineRTPDSCP, MLPPPriorityRTPDSCP, MLPPImmediateRTPDSCP, MLPPFlashRTPDSCP, MLPPFlashOverRTPDSCP, MLPPFlashOverOverRTPDSCP, MLPPNormalizedServiceDomain.

5.8 Configuring the Device to Operate with SNMPv3

This section describes the SNMPv3 configuration process:

- Configuring SNMPv3 using SSH
- Configuring SNMPv3 using EMS (non-configured SNMPv3 System)
- Configuring SNMPv3 using EMS (pre-configured SNMPv3 System)

Note: After configuring SNMPv3, ensure that you disable IPSec.

5.8.1 Configuring SNMPv3 using SSH

The procedure below describes how to configure SNMPv3 using SSH. This is a more secure way of configuring the SNMPv3 connection between the EMS and the device, i.e., before you have a secure SNMP connection, there could be eavesdropping.

➢ **To configure the device to operate with SNMPv3 via SSH:**

1. Open an SSH Client session (e.g. PuTTY), and then connect, using the default user name and password ("Admin" - case sensitive) to the device. If a message appears with the RSA host key, click “Yes” to continue. Verify that the shell prompt appears (“\> ”).
2. Type **Conf**, and then press Enter.
   ```
   /CONFiguration>
   ```
3. Type **cf set**, and then press Enter; the following prompt is displayed:
   ```
   Enter data below. Type a period (.) on an empty line to
   finish.
   ```
   The configuration session is now active and all data entered at the terminal is parsed as configuration text (formatted as an *ini* file).
4. Type the following text at the configuration session:
   ```
   [ SNMPUsers ]
   FORMAT SNMPUsers_Index = SNMPUsers_Username,
   SNMPUsers_AuthProtocol, SNMPUsers_PrivProtocol,
   SNMPUsers_AuthKey, SNMPUsers_PrivKey, SNMPUsers_Group;
   SNMPUsers 0 = v3user, 2, 1,<auth password>,<priv password>, 1;
   [ \SNMPUsers ]
   ```
   where:
   - <auth password> is the password for the for the authentication protocol
   - <priv password> is the password for the privacy protocol

   Possible values for AuthProtocol:
   - 0 – none
   - 1 - MD5
   - 2 - SHA-1

   Possible values for PrivProtocol:
   - 0 – none
   - 1 – DES
   - 3 - AES128

5. To end the PuTTY configuration session, type a full-stop (".") on an empty line; the device responds with the following:

```
INI File replaced
```

6. To save the configuration to the non-volatile memory, type **sar**; the device reboots with IPSec enabled.

5.8.2 Configuring EMS to Operate with a Pre-configured SNMPv3 System

The procedure below describes how to configure the device with a pre-configured SNMPv3.

➢ **To configure EMS to operate with a pre-configured SNMPv3 system:**

1. In the MG Tree, select the required Region to which the device belongs, and then right-click the device.
2. From the shortcut menu, choose **Details**; the 'MG Information' screen appears.

Figure 5-8: MG Information Screen

3. Select the **SNMPv3** option, configure the SNMP fields, and then click **OK**.
4. Open the 'SNMPv3 Users' screen (**Navigation** pane > **System** > **Management** > **SNMP Frame** > **SNMPv3 Users** tab).
5. From the **SNMPv3 Users** tab's drop-down list, choose **Unit value**; the 'SNMPv3 Users' table is refreshed with the values that you entered in Step 3.
6. Click the **Save** button; the EMS and the device are now synchronized.

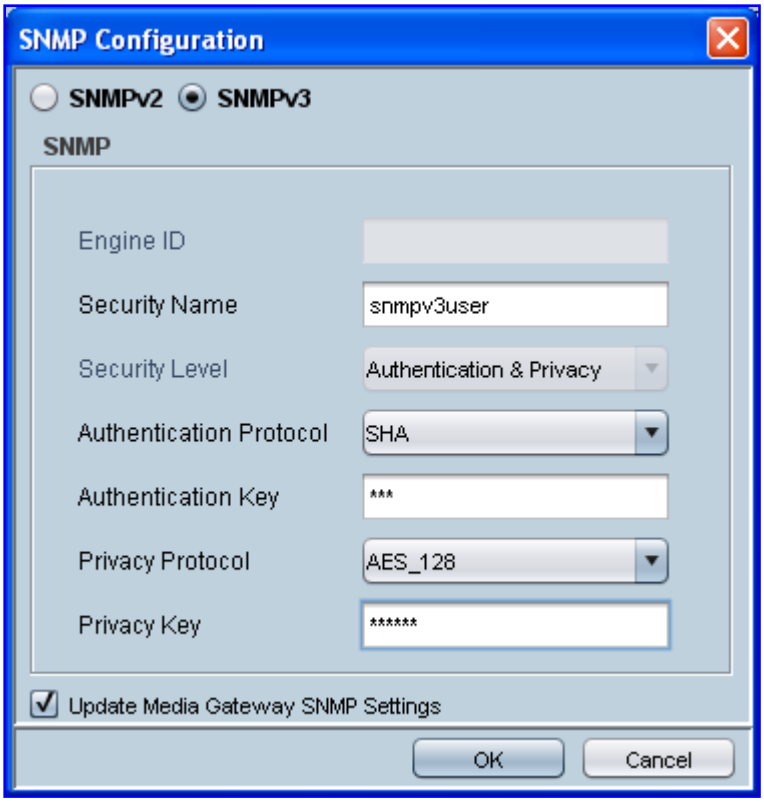
5.8.3 Configuring SNMPv3 to Operate with Non-Configured SNMPv3 System

The procedure below describes how to configure SNMPv3 using the EMS.

➢ **To configure the device to operate with SNMPv3 via EMS (to a non-configured System):**

1. In the MG Tree, select the required Region to which the device belongs; the device is displayed in the Main pane.
2. Right-click the device, and then from the shortcut menu, point to **Configuration**, and then click **SNMP Configuration**; the 'SNMP Configuration' window appears.

Figure 5-9: SNMP Configuration Screen



3. Select the **SNMPv3** option.
4. Configure the SNMPv3 fields, and then select the **Update Media Gateway SNMP Settings** check box.
5. Click **OK**; the update progress is displayed.
6. Click **Done** when complete.
7. Open the 'SNMPv3 Users' screen (**Navigation** pane > **System** > **Management** > **SNMP Frame** > **SNMPv3 Users** tab).
8. From the **SNMPv3 Users** tab's drop-down list, choose **Unit value**; the 'SNMPv3 Users' table is refreshed with the values that you entered in Step 4.
9. Click the **Save** button; the EMS and the device are now synchronized.

5.8.4 Cloning SNMPv3 Users

According to the SNMPv3 standard, SNMPv3 users on the SNMP Agent (on the device) cannot be added via the SNMP protocol, e.g. SNMP Manager (i.e., the EMS). Instead, new users must be defined by User Cloning. The SNMP Manager creates a new user according to the original user permission levels.

➢ **To clone SNMPv3 Users:**

1. Open the 'SNMPv3 Users' screen (**Navigation** pane > **System** > **Management** > **SNMP Frame** > **SNMPv3 Users** tab).
2. Select the user with which you wish to clone permission levels.
3. Click the button; the 'New SNMPv3 User' window appears.
4. Provide a new user name, old passwords of the user you clone permissions from and new user passwords.
5. Select a User permission group.
6. If the new user wishes to receive traps to the user-defined destination, select the **Use SNMPv3 User Security Profile for Trap Forwarding** option to provision Trap destination IP and Port. EMS adds this new user to the SNMP Trap Managers Table. It is also possible to define an additional trap destination after a new user is defined.

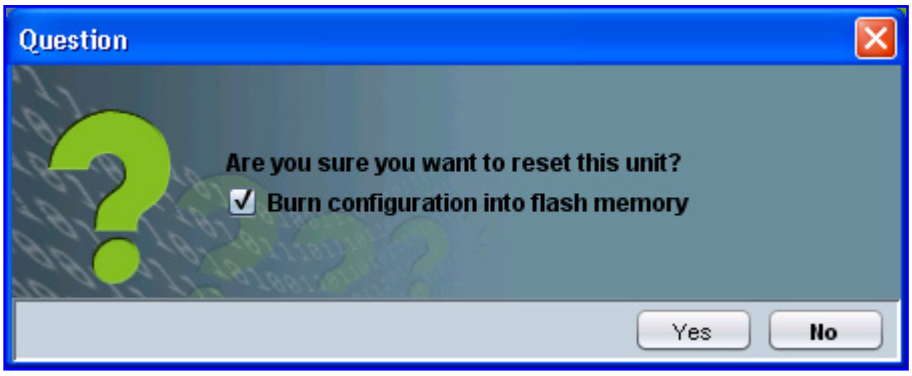
5.9 Resetting the Device

When you have completed configuring the device, you need to save your settings to the device's flash memory and reset the device.

➢ **To save configuration and reset the device:**

1. In the MG Tree, select the device that you want to reset.
2. On the Actions bar, click the **Reset** button.

Figure 5-10: Confirmation for Saving Configuration and Resetting Device



3. Ensure that the option **Burn Configuration into flash memory** is selected.
4. Click **Yes**; the progress of the reset process is displayed.
5. Click **Done** when complete.

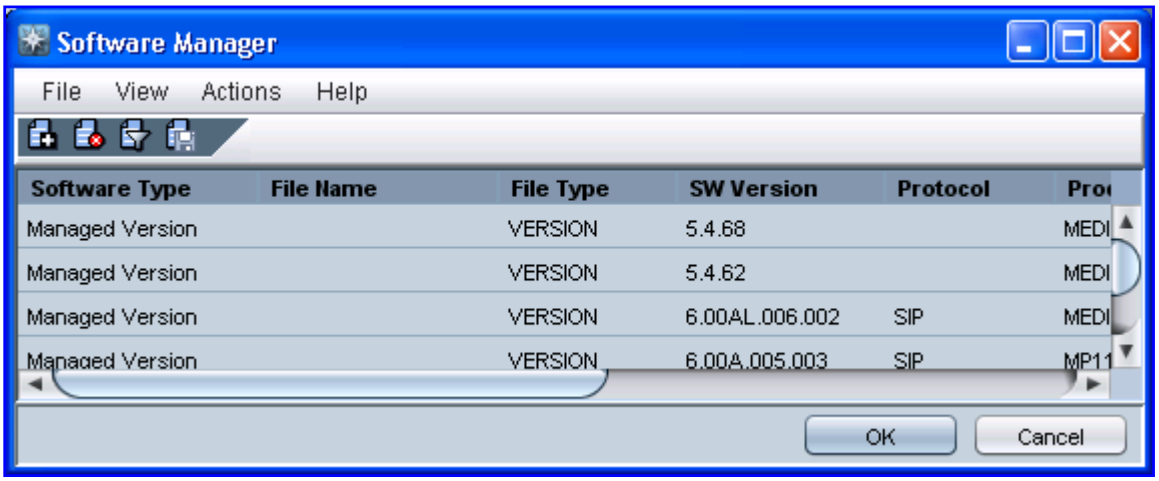
5.10 Upgrading the Device's Software

The procedure below describes how to upgrade the devices software (i.e., cmp file) using the EMS.

➢ **To upgrade the device's cmp file:**

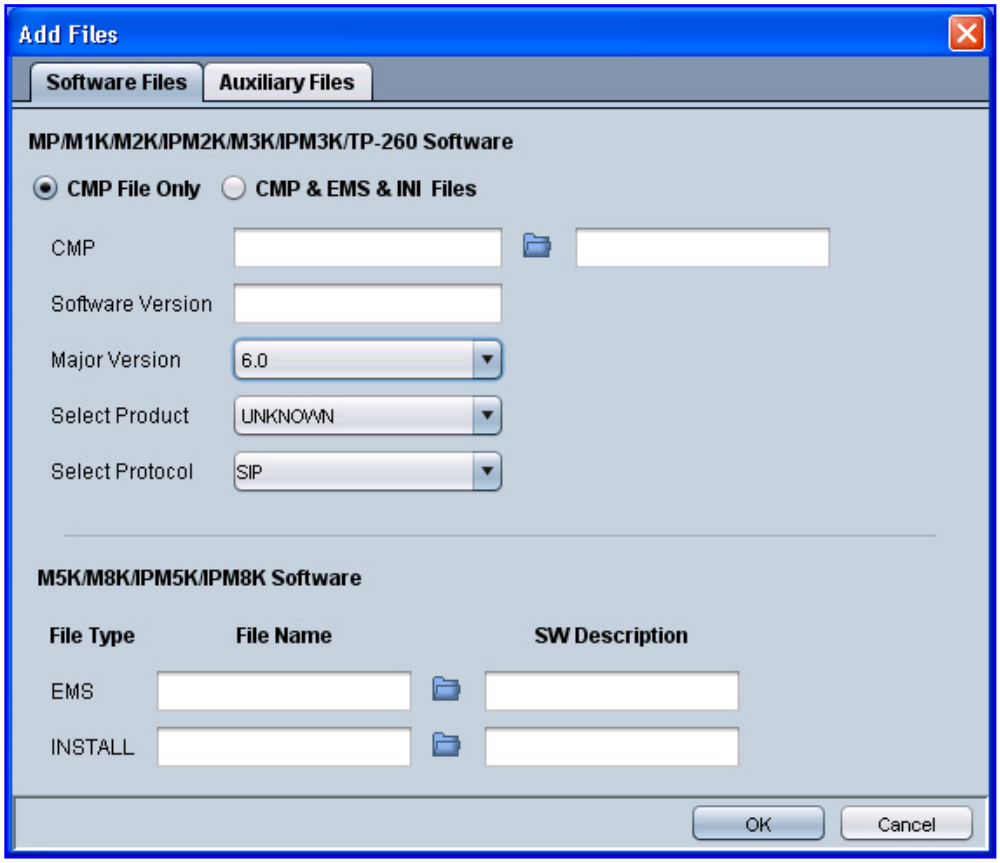
1. From the **Tools** menu, choose **Software Manager**; the 'Software Manager' screen appears.

Figure 5-11: Software Manager Screen



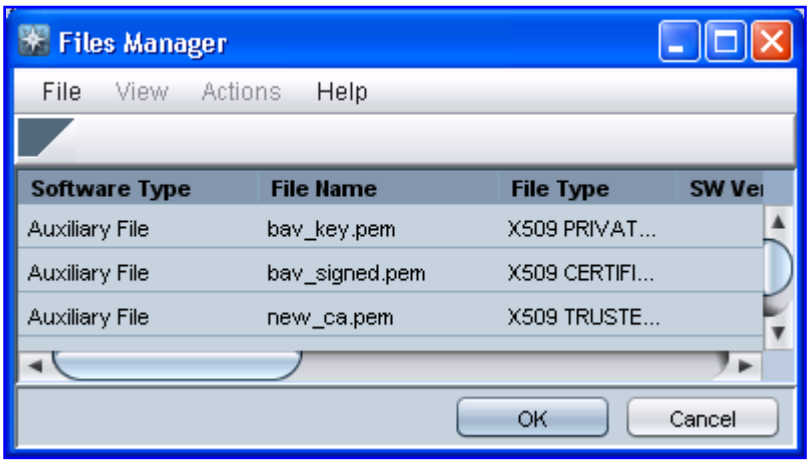
2. Click the **Add File** icon; the 'Add Files' dialog box appears.

Figure 5-12: Add Files Screen



3. Select the cmp file, by performing the following:
   a. Ensure that the **CMP File Only** option is selected.
   b. In the 'CMP' field, click the browse button and navigate to the required cmp file; the software version number of the selected file appears in the 'Software Version' field.
   c. From the 'Major Version' drop-down list, select the version number of the cmp file.
   d. From the 'Select Product' drop-down list, select the type of device.
   e. From the 'Select Protocol' drop-down list, select the control protocol (i.e., SIP).
4. Click **OK**.
5. In the MG Tree, select the device that you want to upgrade.
6. On the Actions bar, click the **Software Upgrade** button; the 'Files Manager' screen appears.

Figure 5-13: Files Manager Screen



7. Select the file that you want to download to the device, and then click **OK**; a confirmation box appears.
8.
9. Click **Yes** to confirm download; the 'Software Download' screen appears, displaying the download progress.
10. Click **Done** when download is completed successfully.

Reader's Notes

6 Restoring Factory Default Settings

You can restore the device's configuration to factory defaults using one of the following methods:

- Using the CLI (see "Restoring Defaults using CLI" on page 215)
- Loading an empty *ini* file (see "Restoring Defaults using an ini File" on page 216)
- Using the hardware Reset button (see Restoring Defaults using Hardware Reset Button on page 216)

6.1 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 device's CLI:
   a. Connect the device's RS-232 port (refer to the *Installation Manual*) to COM1 or COM2 communication port on your PC.
   b. Establish serial communication with the device, using a serial communication program (such as HyperTerminal™) with the following communication port settings:
      - **Baud Rate:** 9,600 bps for MP-11x; 115,200 bps for MP-124
      - **Data Bits:** 8
      - **Parity:** None
      - **Stop Bits:** 1
      - **Flow Control:** None
2. At the CLI prompt, type the following command to access the configuration mode, and then press the Enter key:

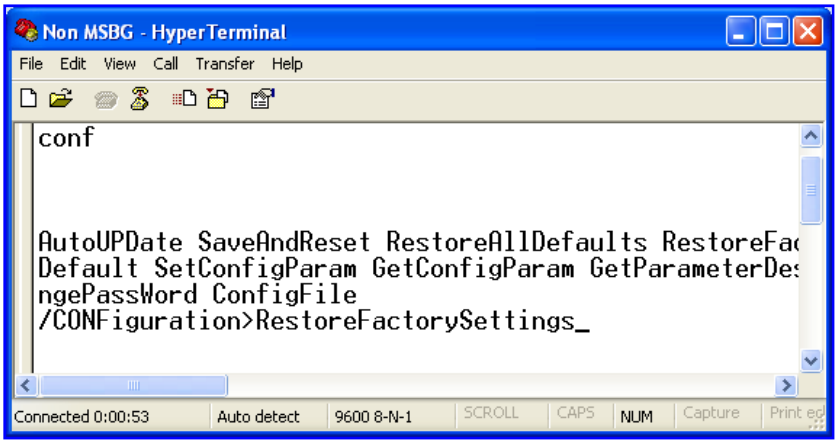
```
conf
```

3. At the prompt, type the following command to reset the device to default settings, and then press the Enter key:

```
RestoreFactorySettings
```

The CLI commands are shown in the terminal emulation program (e.g., HyperTerminal) below:

Figure 6-1: RestoreFactorySettings CLI Command



6.2 Restoring Defaults using an ini File

You can restore the device to factory default settings by loading an empty *ini* file to the device, using the Web interface's 'Configuration File' page (see "Backing Up and Loading Configuration File" on page 178). 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. The loaded *ini* file must be empty (i.e., contain no parameters), or include only comment signs (i.e., semicolons ";") preceding lines (parameters). The default values assigned to the parameters are according to the *cmp* file running on the device.

6.3 Restoring Defaults using Hardware Reset Button

The device's hardware Reset pinhole button can be used to reset the device to default settings. For a detailed description, refer to the *Installation Manual*.

7 Auxiliary Configuration Files

This section describes the auxiliary files that can be loaded to the device:

- Call Progress Tones (see "Call Progress Tones File" on page 217
- Distinctive Ringing in the ini file (see Distinctive Ringing on page 220)
- Prerecorded Tones (see "Prerecorded Tones File" on page 222
- Dial Plan (see Dial Plan File on page 223)
- User Information (see "User Information File" on page 224)

You can load these auxiliary files to the device using one of the following methods:

- Loading the files directly to the device using the device's Web interface (see "Loading Auxiliary Files" on page 170).
- Specifying the auxiliary file name in the *ini* file (see "Auxiliary and Configuration Files Parameters" on page 496) and then loading the *ini* file to the device. The Auxiliary files listed in the *ini* file are then uploaded to the device 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.

7.1 Call Progress Tones File

The Call Progress Tones (CPT) and Distinctive Ringing 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 220).

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 the TrunkPack Downloadable Conversion Utility (DConvert). For a description on converting a CPT *ini* file into a binary *dat* file, refer to the *Product Reference Manual*.

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
    - **[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
```

7.1.1 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
```

7.1.2 FXS Distinctive Ringing and Call Waiting Tones per Source/Destination Number

The device supports the configuration of 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/s depending on the source and/or destination number of the received call. This configuration is performed using the ToneIndex *ini* file table parameter, which maps Ringing and/or Call Waiting tones to source and/or destination number prefixes per FXS endpoint/s.

Typically, the Ringing and/or Call Waiting tone played 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.

For example, to configure Distinctive Ringing and Call Waiting tones of Index #9 in the CPT file for FXS endpoints 1 to 4 when a call is received from a source number with prefix 2, configure the following in the *ini* file:

```
[ToneIndex]
FORMAT ToneIndex Index = ToneIndex FXSPort First,
ToneIndex FXSPort Last, ToneIndex SourcePrefix,
ToneIndex_DestinationPrefix, ToneIndex_PriorityIndex;
ToneIndex_Index 0 = 0, 3, 2, , 1;
[\ToneIndex]
FirstCallWaitingToneID=8
```

Note that the Call Waiting tone index equals to the priority index plus FirstCallWaitingToneID(*). For example, if you want to select the Call Waiting tone defined in the CPT file at Index #9, then you can enter 1 as the priority index and the value 8 for FirstCallWaitingToneID. The summation of these values equals 9, i.e., index #9.

7.2 Prerecorded Tones File

The CPT file mechanism has several limitations such as a limited number of predefined tones and a limited number of frequency integrations in one tone. To overcome these limitations and provide tone generation capability that is more flexible, the Prerecorded Tones (PRT) file can be used. If a specific prerecorded tone exists in the PRT file, it takes precedence over the same tone that exists in the CPT file and is played instead of it.

Note: The PRT are used only for generation of tones. Detection of tones is performed according to the CPT file.

The PRT is a **.dat* file containing a set of prerecorded tones that can be played by the device. Up to 40 tones (totaling approximately 10 minutes) can be stored in a single PRT file on the device's flash memory. The prerecorded tones are prepared offline using standard recording utilities (such as CoolEdit™) and combined into a single file using the DConvert utility (refer to the *Product Reference Manual*).

The raw data files must be recorded with the following characteristics:

- **Coders:** G.711 A-law or G.711 µ-law
- **Rate:** 8 kHz
- **Resolution:** 8-bit
- **Channels:** mono

Once created, the PRT file can then be loaded to the device using AudioCodes' BootP/TFTP utility or the Web interface (see "Loading Auxiliary Files" on page 170).

The prerecorded tones are played repeatedly. This allows you to record only part of the tone and then play the tone for the full duration. For example, if a tone has a cadence of 2 seconds on and 4 seconds off, the recorded file should contain only these 6 seconds. The PRT module repeatedly plays this cadence for the configured duration. Similarly, a continuous tone can be played by repeating only part of it.

7.3 Dial Plan File

The Dial Plan file contains a list of up to eight dial plans, supporting a total of up to 8,000 user-defined, distinct prefixes (e.g. area codes, international telephone number patterns) for the PSTN to which the device is connected. The Dial Plan is used for the following:

- (Tel-to-IP calls): The file includes up to eight patterns (i.e., eight dial plans). These allow the device to know when digit collection ends, after which it starts sending all the collected (or dialed) digits (in the INVITE message). This also provides enhanced digit mapping.

The Dial Plan file is first created using a text-based editor (such as Notepad) and saved with the file extension *.ini. This *ini* file is then converted to a binary file (*.dat) using the DConvert utility (refer to the *Product Reference Manual*). Once converted, it can then be loaded to the device using the Web interface (see "Loading Auxiliary Files" on page 170).

The Dial Plan file must be prepared in a textual *ini* file with the following syntax:

- Every line in the file defines a known dialing prefix and the number of digits expected to follow that prefix. The prefix must be separated from the number of additional digits by a comma (',').
- Empty lines are ignored.
- Lines beginning with a semicolon (';') are ignored.
- Multiple dial plans may be specified in one file; a name in square brackets on a separate line indicates the beginning of a new dial plan. Up to eight dial plans can be defined.
- Asterisks ('*') and number-signs ('#') can be specified as part of the prefix.
- Numeric ranges are allowed in the prefix.
- A numeric range is allowed in the number of additional digits.

Notes:

- The prefixes must not overlap. Attempting to process an overlapping configuration by the DConvert utility results in an error message specifying the problematic line.
- For a detailed description on working with Dial Plan files, see "External Dial Plan File" on page 230.

An example of a Dial Plan file in *ini*-file format (i.e., before converted to *.dat) that contains two dial plans is shown below:

```
; Example of dial-plan configuration.
; This file contains two dial plans:
[ PLAN1 ]
; Defines cellular/VoIP area codes 052, 054, and 050.
; In these area codes, phone numbers have 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
```

7.4 User Information File

The User Information file is a text file that maps PBX extensions connected to the device to global IP numbers. In this context, a global IP phone number (alphanumerical) serves as a routing identifier for calls in the 'IP world'. The PBX extension uses this mapping to emulate the behavior of an IP phone.

Note: By default, the mapping mechanism is disabled and must be activated using the parameter EnableUserInfoUsage.

The maximum size of the file is 10,800 bytes. Each line in the file represents a mapping rule of a single PBX extension. Up to 100 rules can be configured. Each line includes five items separated with commas. The items are described in the table below:

Table 7-1: User Information Items

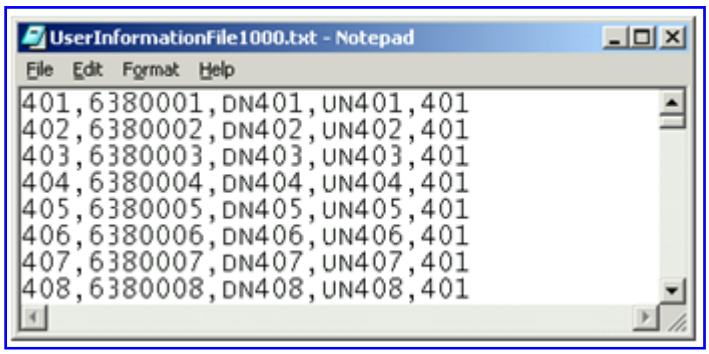
Item	Description	Maximum Size (Characters)
PBX extension #	The relevant PBX extension number.	10
Global phone #	The relevant global phone number.	20
Display name	A string that represents the PBX extensions for the Caller ID.	30

Item	Description	Maximum Size (Characters)
Username	A string that represents the user name for SIP registration.	40
Password	A string that represents the password for SIP registration.	20

Note: For FXS ports, when the device is required to send a new request with the 'Authorization' header (for example, after receiving a SIP 401 reply), it uses the user name and password from the Authentication table. To use the username and password from the User Info file, change the parameter 'Password' from its default value.

An example of a User Information file is shown in the figure below:

Figure 7-1: Example of a User Information File



Note: The last line in the User Information file must end with a carriage return (i.e., by pressing the <Enter> key).

The User Information file can be loaded to the device by using one of the following methods:

- *ini* file, using the parameter UserInfoFileName (described in "Auxiliary and Configuration Files Parameters" on page 496)
- Web interface (see "Loading Auxiliary Files" on page 170)
- Automatic update mechanism, using the parameter UserInfoFileURL (refer to the *Product Reference Manual*)

Each PBX extension registers separately (a REGISTER message is sent for each entry only if AuthenticationMode is set to Per Endpoint) using the"Global phone number" in the From/To headers. The REGISTER messages are sent gradually. Initially, the device sends requests according to the maximum number of allowed SIP dialogs (configured by the parameter NumberOfActiveDialogs). After each received response, the subsequent request is sent. Therefore, no more than NumberOfActiveDialogs dialogs are active simultaneously. The user name and password are used for SIP Authentication when required.

The calling number of outgoing Tel-to-IP calls is translated to a "Global phone number" only after Tel-to-IP manipulation rules (if defined) are performed. The Display Name is used in the From header in addition to the "Global phone number". The called number of incoming IP-to-Tel calls is translated to a PBX extension only after IP-to-Tel manipulation rules (if defined) are performed.

8 IP Telephony Capabilities

This section describes the device's main IP telephony capabilities.

8.1 Dynamic Jitter Buffer Operation

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. In many cases, however, some frames can 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 using the following parameters:

- **Minimum delay:** DJBufMinDelay (0 msec to 150 msec)
  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:** DJBufOptFactor (0 to 12, 13)
  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.

For 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.

8.2 Gateway and IP-to-IP

This section describes various Gateway and IP-to-IP application features.

8.2.1 Dialing Plan Features

This section discusses various dialing plan features supported by the device:

- Dialing plan notations (see "Dialing Plan Notation for Routing and Manipulation" on page 228)
- Digit mapping (see "Digit Mapping" on page 229)
- External Dial Plan file containing dial plans (see "External Dial Plan File" on page 230)

8.2.1.1 Dialing Plan Notation for Routing and Manipulation

The device supports flexible dialing plan notations for representing digits (single or multiple) entered for destination and source prefixes (of phone numbers and SIP URI user names) in the routing and manipulation tables.

Table 8-1: Dialing Plan Notations

Notation	Description	Example
[n-m]	Represents a range of numbers. **Note:** Range of letters is not supported.	▪ **[5551200-5551300]#:** represents all numbers from 5551200 to 5551300. ▪ **123[100-200]:** represents all numbers from 123100 to 123200.
[n,m,...]	Represents multiple numbers. Up to three digits can be used to denote each number.	▪ **[2,3,4,5,6]#:** represents a one-digit number starting with 2, 3, 4, 5, or 6. ▪ **[11,22,33]xxx#:** represents a five-digit number that starts with 11, 22, or 33. ▪ **[111,222]xxx#:** represents a six-digit number that starts with 111 or 222.
[n1-m1,n2-m2,a,b,c,n3-m3]	Represents a mixed notation of multiple ranges and single numbers. **Note:** The ranges and the single numbers must have the same number of digits. For example, each number range and single number in the dialing plan [123-130,455,577,780-790] consists of three digits.	**[123-130,455,766,780-790]:** represents numbers 123 to 130, 455, 766, and 780 to 790.
x	Represents any single digit.	-
Pound sign (#) at the end of a number	Represents the end of a number.	**54324xx#:** represents a 7-digit number that starts with 54324.
A single asterisk (*)	Represents any number.	***:** represents any number (i.e., all numbers).

8.2.1.2 Digit Mapping

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:

Table 8-2: Digit Map Pattern Notations

Notation	Description
[n-m]	Range of numbers (not letters).
.	(single dot) Repeat digits until next notation (e.g., T).
x	Any single digit.
T	Dial timeout (configured by the TimeBetweenDigits parameter).
S	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|91xxxxxxxxxx|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 "External Dial Plan File" on page 230), 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.

8.2.1.3 External Dial Plan File

The device allows you to select a specific Dial Plan (index) defined in an external Dial Plan file. This file is loaded to the device as a *.dat file (binary file), converted from an *ini* file using the DConvert utility. This file can include up to eight Dial Plans (Dial Plan indices), with a total of up to 8,000 dialing rules (lines). The required Dial Plan is selected using the DialPlanIndex parameter. This parameter can use values 0 through 7, where 0 denotes PLAN1, 1 denotes PLAN2, and so on. The Dial Plan index can be configured globally or per Tel Profile.

The format of the Dial Plan index file is as follows:

- A name in square brackets ("[...]") on a separate line indicates the beginning of a new Dial Plan index.
- Every 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 asterisks ("*") and number signs ("#").
- The number of additional digits can include a numerical range in the format x-y.
- Empty lines and lines beginning with a semicolon (";") are ignored.

An example of a Dial Plan file with indices (in *ini*-file format before conversion to binary *.dat) is shown below:

```
[ PLAN1 ]
; Area codes 02, 03, - phone numbers include 7 digits.
02,7
03,7
; Cellular/VoIP area codes 052, 054 - phone numbers include 8
digits.
052,8
054,8
; International prefixes 00, 012, 014 - number following
prefix includes 7 to 14 digits.
00,7-14
012,7-14
014,7-14
; Emergency number 911 (no additional digits expected).
911,0
[ PLAN2 ]
; Supplementary services such as Call Camping and Last Calls
(no additional digits expected), by dialing *41, *42, or *43.
*4[1-3],0
```

Notes:

- If you are using an external Dial Plan file for dialing plans (see "External Dial Plan File" on page 230), 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.

8.2.2 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 "Manipulation" on page 129):

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.

Figure 8-1: Prefix to Add Field with Notation

Index	Destination Prefix	Source Prefix	Source IP Address	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add
1	+5492028888888	*	*	7	0	0[5,3]15

In this configuration, the following manipulation process occurs: 1) the prefix is calculated, 020215 in the example; 2) the first seven digits from the left are removed from the original number, in the example, the number is changed to 8888888; 3) the prefix that was previously calculated is then added.

8.2.3 Configuring DTMF Transport Types

You can control the way DTMF digits are transported over the IP network to the remote endpoint, by using one of the following modes:

- **Using INFO message according to Nortel IETF draft:** DTMF digits are carried to the remote side in INFO messages. To enable this mode, define the following:
  - RxDTMFOption = 0
  - TxDTMFOption = 1

  Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0).
- **Using INFO message according to Cisco's mode:** DTMF digits are carried to the remote side in INFO messages. To enable this mode, define the following:
  - RxDTMFOption = 0
  - TxDTMFOption = 3

  Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0).
- **Using NOTIFY messages according to IETF Internet-Draft draft-mahy-sipping-signaled-digits-01**: DTMF digits are carried to the remote side using NOTIFY messages. To enable this mode, define the following:
  - RxDTMFOption = 0
  - TxDTMFOption = 2

  Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0).
- **Using RFC 2833 relay with Payload type negotiation:** DTMF digits are carried to the remote side as part of the RTP stream in accordance with RFC 2833 standard. To enable this mode, define the following:
  - RxDTMFOption = 3
  - TxDTMFOption = 4

  Note that to set the RFC 2833 payload type with a different value (other than its default), configure 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 the RFC2833PayloadType 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:
  - RxDTMFOption = 0 (i.e., disabled)
  - TxDTMFOption = 0 (i.e., disabled)
  - DTMFTransportType = 2 (i.e., transparent)
- **Using INFO message according to Korea mode:** DTMF digits are carried to the remote side in INFO messages. To enable this mode, define the following:
  - RxDTMFOption = 0 (i.e., disabled)
  - TxDTMFOption = 3

  Note that in this mode, DTMF digits are erased from the audio stream (DTMFTransportType is automatically set to 0).

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 RxDTMFOption to 0 in the *ini* file.

The following parameters affect the way the device handles the DTMF digits:

- TxDTMFOption, RxDTMFOption, and RFC2833PayloadType
- MGCPDTMFDetectionPoint, DTMFVolume, DTMFTransportType, DTMFDigitLength, and DTMFInterDigitInterval

8.2.4 FXS and FXO Capabilities

8.2.4.1 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 types can be selected using the *ini* file parameters FXSCountryCoefficients (for FXS) and CountryCoefficients (for FXO), or using the Web interface (see "Configuring Analog Settings" on page 101).

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

8.2.4.2 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 235)
- For Tel-to-IP calls (see "FXO Operations for Tel-to-IP Calls" on page 238)
- Call termination on FXO devices (see "Call Termination on FXO Devices" on page 240)

8.2.4.2.1 FXO Operations for IP-to-Tel Calls

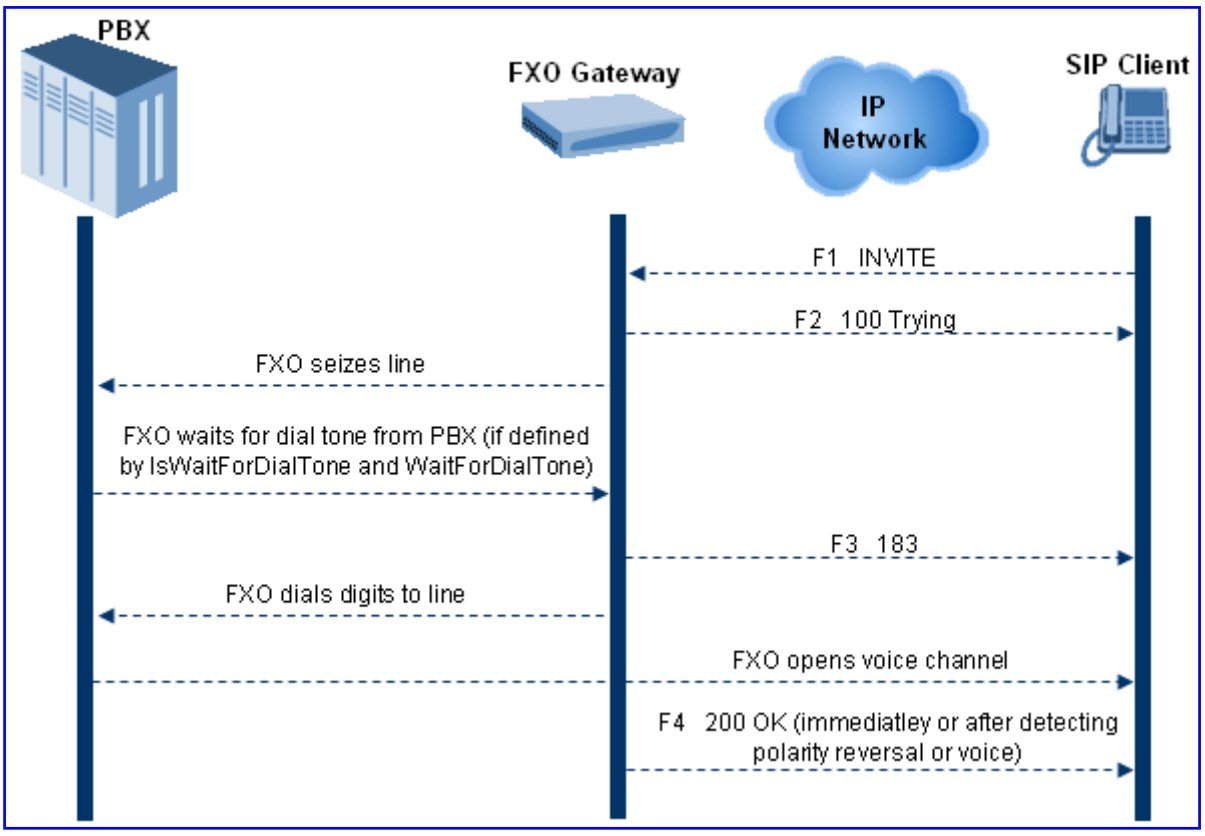
The FXO device provides the following operating modes for IP-to-Tel calls:

- One-stage dialing (see "One-Stage Dialing" on page 235)
  - Waiting for dial tone (see "Two-Stage Dialing" on page 236)
  - Time to wait before dialing
  - Answer supervision
- Two-stage dialing (see "Two-Stage Dialing" on page 236)
- Dialing time: DID wink (see "DID Wink" on page 237)

8.2.4.2.1.1 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.

Figure 8-2: Call Flow for One-Stage Dialing



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.

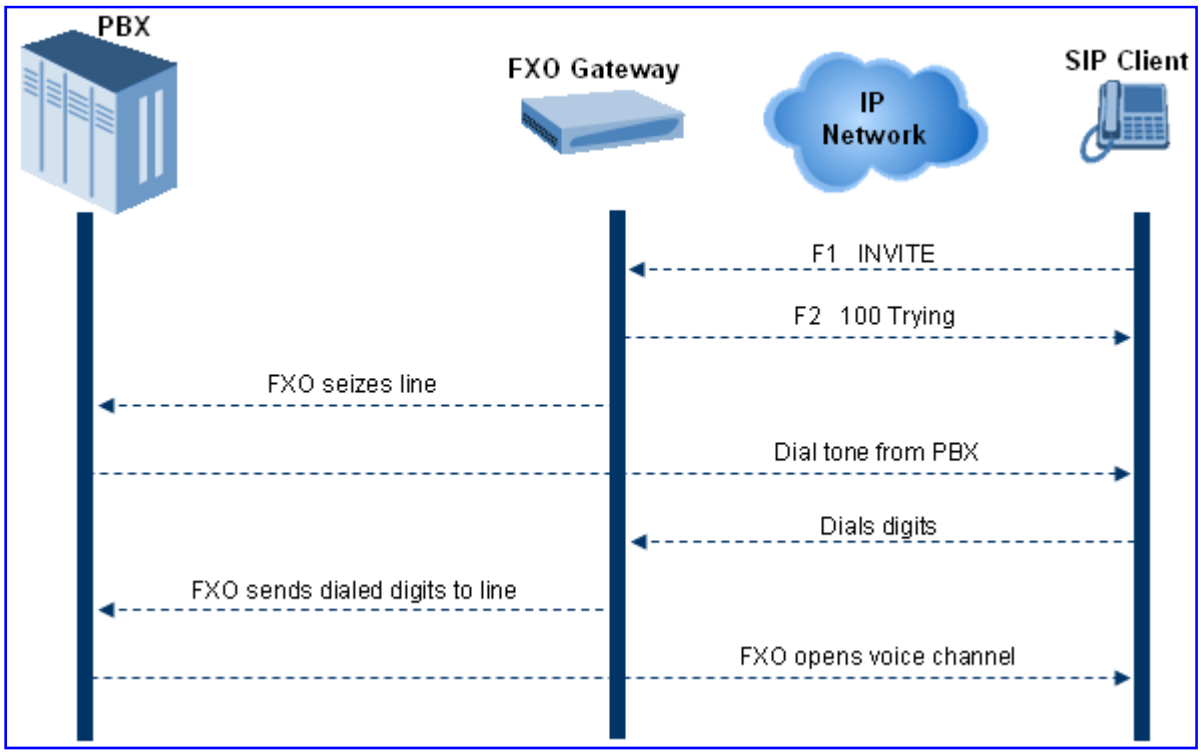
Note: The *ini* file parameter IsWaitForDialTone must be disabled for this mode.

- **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: device sends a 200 OK in response to an INVITE only when it detects a polarity reversal.
  - Voice Detection: device sends a 200 OK in response to an INVITE only when it detects the start of speech (or ringback tone) from the Tel side. (Note that the IPM detectors must be enabled).

8.2.4.2.1.2 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 8-3: 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

8.2.4.2.1.3 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

8.2.4.2.2 FXO Operations for Tel-to-IP Calls

The FXO device provides the following FXO operating modes for Tel-to-IP calls:

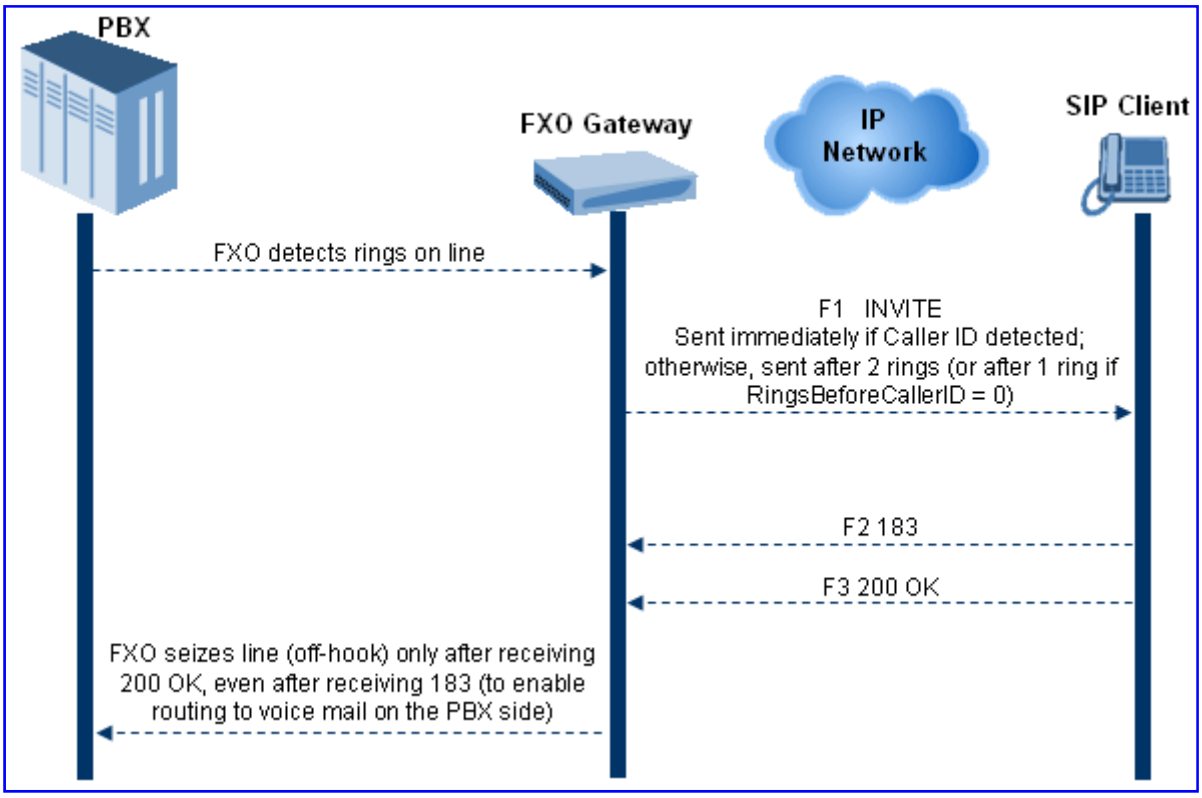
- Automatic Dialing (see "Automatic Dialing" on page 238)
- Collecting Digits Mode (see "Collecting Digits Mode" on page 239)
- FXO Supplementary Services (see "FXO Supplementary Services" on page 239)
  - Hold/Transfer Toward the Tel side
  - Hold/Transfer Toward the IP side
  - Blind Transfer to the Tel side

8.2.4.2.2.1 Automatic Dialing

Automatic dialing is defined using the *ini* file parameter table TargetOfChannel (see Analog Telephony Parameters) or the embedded Web server's 'Automatic Dialing' screen (see "Automatic Dialing" on page 154).

The SIP call flow diagram below illustrates Automatic Dialing.

Figure 8-4: Call Flow for Automatic Dialing

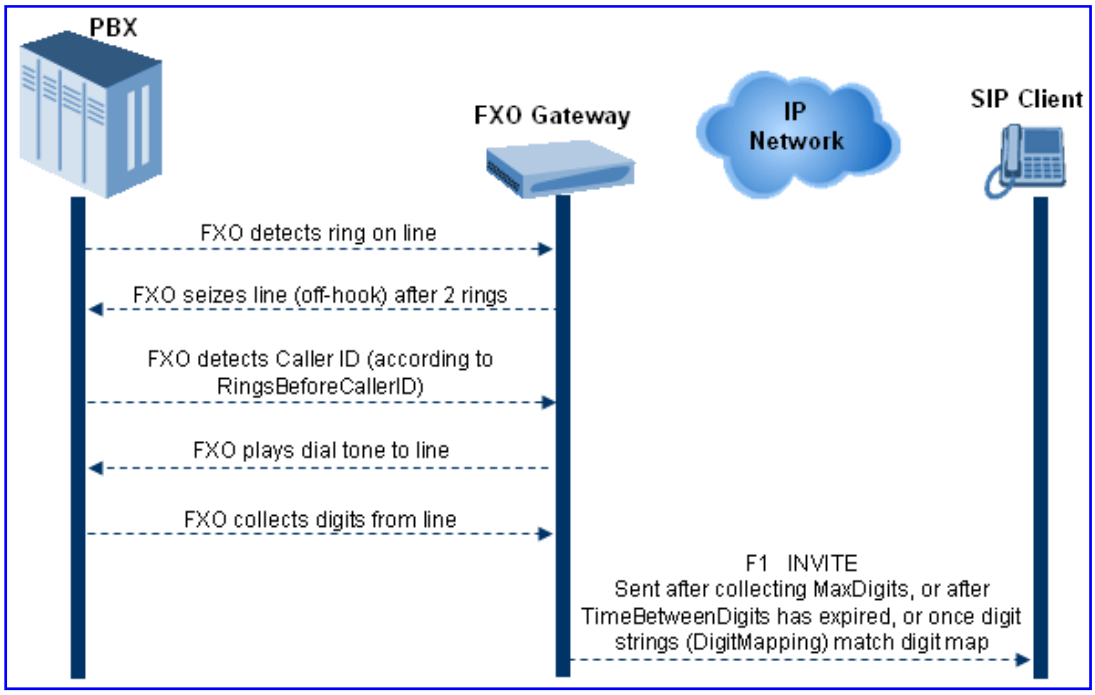


8.2.4.2.2.2 Collecting Digits Mode

When automatic dialing is not defined, the device collects the digits.

The SIP call flow diagram below illustrates the Collecting Digits Mode.

Figure 8-5: Call Flow for Collecting Digits



8.2.4.2.2.3 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.

8.2.4.2.3 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 240)
- Calls terminated before call establishment (see "Call Termination before Call Establishment" on page 241)
- Ring detection timeout (see "Ring Detection Timeout" on page 241)

8.2.4.2.3.1 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 not known, define them in the CPT file (the tone produced by the PBX / CO must be recorded and its frequencies analyzed -- refer to Adding a Reorder Tone to the CPT File in the Reference Manual). This method is slightly less reliable than the previous one. You can use the CPTWizard (described in the *Reference Manual*) 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.

8.2.4.2.3.2 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.

8.2.4.2.3.3 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).

8.2.4.3 Remote PBX Extension Between FXO and FXS Devices

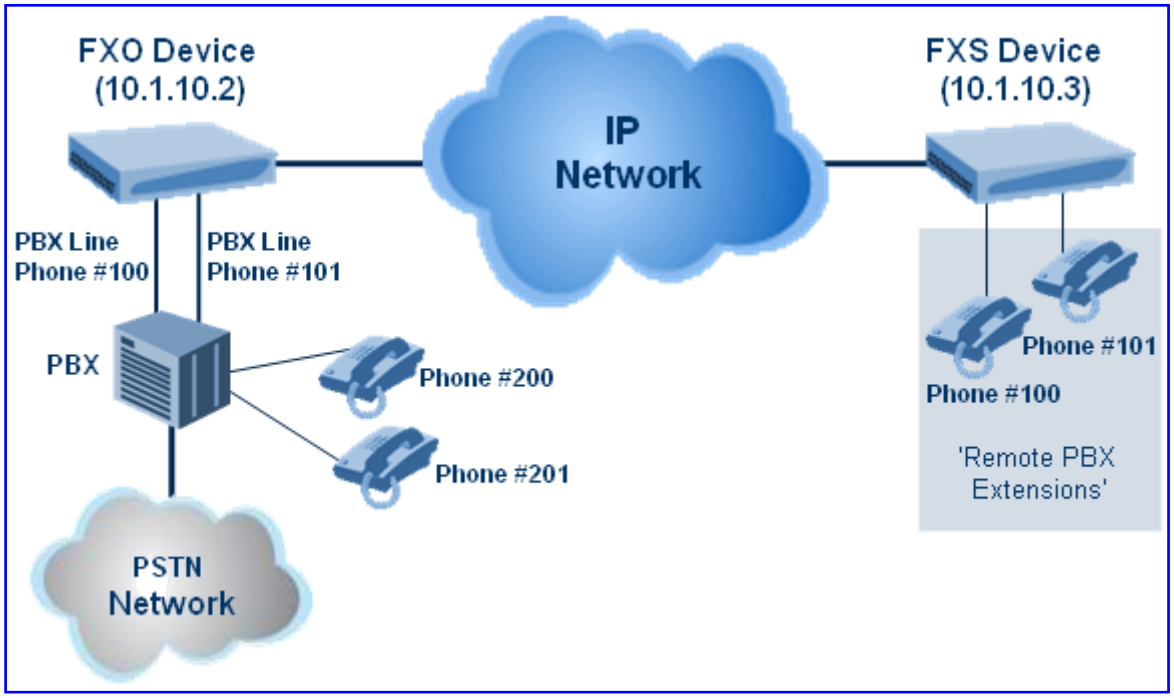
Remote PBX extension offers a company the capability of extending the "power" of its local PBX by allowing remote phones (remote offices) to connect to the company's PBX over the IP network (instead of via PSTN). This is as if the remote office is located in the head office (where the PBX is installed). 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 8-port FXO and 8-port 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:

- One FXO interfaces with ports connected directly to the PBX lines (shown in the figure below)
- One FXS interfaces for the 'remote PBX extension'
- Analog phones (POTS)
- PBX (one or more PBX loop start lines)
- LAN network

Figure 8-6: FXO-FXS Remote PBX Extension (Example)



8.2.4.3.1 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.

8.2.4.3.2 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.

8.2.4.3.3 Message Waiting Indication for Remote Extensions

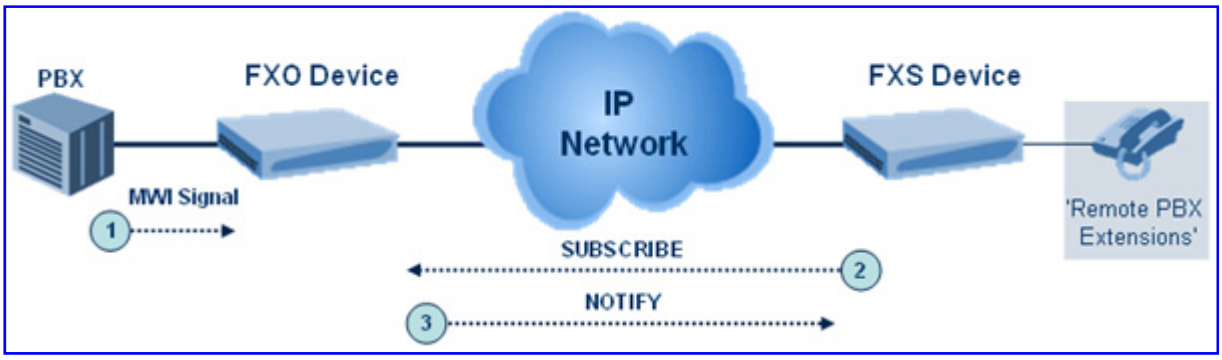
The device supports the relaying of Message Waiting Indications (MWI) for remote extensions (and voice mail applications). Instead of subscribing to an MWI server to receive notifications of pending messages, the FXO device receives subscriptions from the remote FXS device and notifies the appropriate 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.

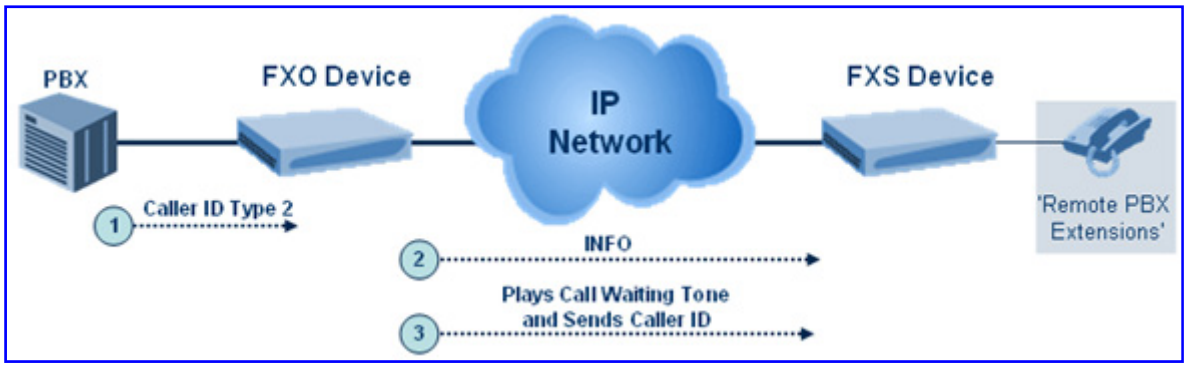
Figure 8-7: MWI for Remote Extensions



8.2.4.3.4 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.

Figure 8-8: Call Waiting for Remote Extensions



8.2.4.3.5 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 'Endpoint Phone Numbers' page (see Configuring Endpoint Phone Numbers on page 124, assign the phone numbers 100 to 107 to the device's endpoints.

Figure 8-9: Assigning Phone Numbers to FXS Endpoints

	Channel(s)	Phone Number	Hunt Group ID
1	1-8	100	
2			

2. In the 'Automatic Dialing' page (see "Configuring Automatic Dialing" on page 154), 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 8-10: Automatic Dialing for FXS Ports

Gateway Port	Destination Phone Number	Auto Dial Status
Port 1 FXS	200	Enable
Port 2 FXS	201	Enable
Port 3 FXS	202	Enable
Port 4 FXS	203	Enable
Port 5 FXS	204	Enable
Port 6 FXS	205	Enable
Port 7 FXS	206	Enable
Port 8 FXS	206	Enable

3. In the 'Tel to IP Routing' page (see "Configuring Tel to IP Routing" on page 138), enter 20 for the destination phone prefix, and 10.1.10.2 for the IP address of the FXO device.

Figure 8-11: 1. FXS Tel-to-IP Routing Configuration

	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).

8.2.4.3.6 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:**

1. In the 'Endpoint Phone Numbers' page (see Configuring Endpoint Phone Numbers on page 124, assign the phone numbers 200 to 207 to the device's FXO endpoints.

Figure 8-12: Assigning Phone Numbers to FXO Ports

	Channel(s)	Phone Number	Hunt Group ID
1	1-8	200	

2. 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 8-13: FXO Automatic Dialing Configuration

Gateway Port	Destination Phone Number	Auto Dial Status
Port 1 FXO	100	Enable
Port 2 FXO	101	Enable
Port 3 FXO	102	Enable
Port 4 FXO	103	Enable
Port 5 FXO	104	Enable
Port 6 FXO	105	Enable
Port 7 FXO	106	Enable
Port 8 FXO	107	Enable

3. In the 'Tel to IP Routing' 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 8-14: FXO Tel-to-IP Routing Configuration

	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address
1	10	*		10.1.10.3

4. In the 'FXO Settings' page (see "Configuring FXO Parameters" on page 152), set the parameter 'Dialing Mode' to 'Two Stages' (IsTwoStageDial = 1).

8.2.5 Configuring Alternative Routing (Based on Connectivity and QoS)

The Alternative Routing feature enables reliable routing of Tel-to-IP calls when a Proxy isn't used. The device periodically checks the availability of connectivity and suitable Quality of Service (QoS) before routing. If the expected quality cannot be achieved, an alternative IP route for the prefix (phone number) is selected.

The following parameters are used to configure the Alternative Routing mechanism:

- AltRoutingTel2IPEnable
- AltRoutingTel2IPMode
- IPConnQoSMaxAllowedPL
- IPConnQoSMaxAllowedDelay

8.2.5.1 Alternative Routing Mechanism

When the device routes a Tel-to-IP call, the destination number is compared to the list of prefixes defined in the 'Tel to IP Routing' (described in "Configuring the Tel to IP Routing" on page 138). This table is scanned for the destination number's prefix starting at the top of the table. For this reason, you must enter the main IP route above any alternative route in the table. When an appropriate entry (destination number matches one of the prefixes) is found, the prefix's corresponding destination IP address is verified. If the destination IP address is disallowed (or if the original call fails and the device has made two additional attempts to establish the call without success), an alternative route is searched in the table and used for routing the call.

Destination IP address is disallowed if no ping to the destination is available (ping is continuously initiated every seven seconds), when an inappropriate level of QoS was detected or when a DNS host name is not resolved. The QoS level is calculated according to delay or packet loss of previously ended calls. If no call statistics are received for two minutes, the QoS information is reset.

8.2.5.2 Determining the Availability of Destination IP Addresses

To determine the availability of each destination IP address (or host name) in the routing table, one or all of the following user-defined methods are applied:

- Connectivity: The destination IP address is queried periodically (currently only by ping).
- **QoS:** The QoS of an IP connection is determined according to RTCP statistics of previous calls. Network delay (in msec) and network packet loss (in percentage) are separately quantified and compared to a certain (configurable) threshold. If the calculated amounts (of delay or packet loss) exceed these thresholds, the IP connection is disallowed.
- **DNS resolution:** When host name is used (instead of IP address) for the destination route, it is resolved to an IP address by a DNS server. Connectivity and QoS are then applied to the resolved IP address.

8.2.6 Fax and Modem Capabilities

This section describes the device's fax and modem capabilities, and includes the following main subsections:

- Fax and modem operating modes (see "Fax/Modem Operating Modes" on page 248)
- Fax and modem transport modes (see "Fax/Modem Transport Modes" on page 248)
- V.152 support (see "V.152 Support" on page 253)

8.2.6.1 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 253): 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).

8.2.6.2 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 248)
- G.711 Transport: switching to G.711 when fax/modem is detected (see "G.711 Fax / Modem Transport Mode" on page 250)
- Fax fallback to G.711 if T.38 is not supported (see "Fax Fallback" on page 250)
- Fax and modem bypass: a proprietary method that uses a high bit rate coder (see "Fax/Modem Bypass Mode" on page 250)
- NSE Cisco's Pass-through bypass mode for fax and modem (see "Fax / Modem NSE Mode" on page 251)
- Transparent with events: passing the fax / modem signal in the current voice coder with adaptations (see "Fax / Modem Transparent with Events Mode" on page 252)
- Transparent: passing the fax / modem signal in the current voice coder (see "Fax / Modem Transparent Mode" on page 252)
- RFC 2833 ANS Report upon Fax/Modem Detection (see "RFC 2833 ANS Report upon Fax/Modem Detection" on page 253)

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

8.2.6.2.1 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 249)
- 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 249)

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 parameter FaxRelayMaxRate (this parameter doesn't affect the actual transmission rate). In addition, you can enable or disable Error Correction Mode (ECM) fax mode using the FaxRelayECMEnable parameter.

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 FaxRelayRedundancyDepth and FaxRelayEnhancedRedundancyDepth parameters. Although this is a proprietary redundancy scheme, it should not create problems when working with other T.38 decoders.

8.2.6.2.1.1 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 parameter FaxTransportMode is ignored.

To configure T.38 mode using SIP Re-INVITE messages, set IsFaxUsed to 1. Additional configuration parameters include the following:

- FaxRelayEnhancedRedundancyDepth
- FaxRelayRedundancyDepth
- FaxRelayECMEnable
- 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).

8.2.6.2.1.2 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, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 1
- Additional configuration parameters:
  - FaxRelayEnhancedRedundancyDepth
  - FaxRelayRedundancyDepth
  - FaxRelayECMEnable
  - FaxRelayMaxRate

8.2.6.2.2 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.711A-law:** a=gpmd:0 vbd=yes;ecan=on (or off, for modems)
- **For G.711 µ-law:** a=gpmd:8 vbd=yes;ecan=on (or off for modems)

The parameters FaxTransportMode and VxxModemTransportType are ignored and automatically set to the mode called 'transparent with events'.

To configure fax / modem transparent mode, set IsFaxUsed to 2.

8.2.6.2.3 Fax Fallback

In this mode, when the terminating device detects a fax signal, it sends a Re-INVITE message to the originating device with T.38. If the remote device doesn't support T.38 (replies with SIP response 415 'Media Not Supported'), the device sends a new Re-INVITE with G.711 VBD with the following adaptations:

- Echo Canceller = on
- Silence Compression = off
- Echo Canceller Non-Linear Processor Mode = off
- Dynamic Jitter Buffer Minimum Delay = 40
- Dynamic Jitter Buffer Optimization Factor = 13

When the device initiates a fax session using G.711, a 'gpmd' attribute is added to the SDP according to the following format:

- **For G.711A-law:** a=gpmd:0 vbd=yes;ecan=on
- **For G.711 µ-law:** a=gpmd:8 vbd=yes;ecan=on

In this mode, the parameter FaxTransportMode is ignored and automatically set to 'transparent'.

To configure fax fallback mode, set IsFaxUsed to 3.

8.2.6.2.4 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 parameter FaxModemBypassCoderType). In addition, the channel is 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 parameters FaxBypassPayloadType and ModemBypassPayloadType). During the bypass period, the coder uses the packing factor, which is defined by the parameter FaxModemBypassM. The packing factor determines the number of coder payloads (each the size of FaxModemBypassBasicRTPPacketInterval) 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, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 2
- V21ModemTransportType = 2
- V22ModemTransportType = 2
- V23ModemTransportType = 2
- V32ModemTransportType = 2
- V34ModemTransportType = 2
- BellModemTransportType = 2
- Additional configuration parameters:
  - FaxModemBypassCoderType
  - FaxBypassPayloadType
  - ModemBypassPayloadType
  - FaxModemBypassBasicRTPPacketInterval
  - FaxModemBypasDJBufMinDelay

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 G711 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
- FaxModemBypassCoderType = same coder used for voice
- FaxModemBypassM = same interval as voice
- ModemBypassPayloadType = 8 if voice coder is A-Law; 0 if voice coder is Mu-Law

8.2.6.2.5 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 (using NSEpayloadType, usually 100). These packets signal the remote device to switch to G.711 coder (according to the parameter FaxModemBypassCoderType). 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 the proprietary AudioCodes' Bypass mode FaxBypassPayloadType and ModemBypassPayloadType 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, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 2
- NSEMode = 1
- NSEPayloadType = 100
- V21ModemTransportType = 2
- V22ModemTransportType = 2
- V23ModemTransportType = 2
- V32ModemTransportType = 2
- V34ModemTransportType = 2
- BellModemTransportType = 2

8.2.6.2.6 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, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 3
- V21ModemTransportType = 3
- V22ModemTransportType = 3
- V23ModemTransportType = 3
- V32ModemTransportType = 3
- V34ModemTransportType = 3
- BellModemTransportType = 3

8.2.6.2.7 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 the Profiles mechanism (see "Coders and Profile Definitions" on page 117) to apply certain adaptations to the channel used for fax / modem (e.g., 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, use the following parameters:

- IsFaxUsed = 0
- FaxTransportMode = 0
- V21ModemTransportType = 0

- V22ModemTransportType = 0
- V23ModemTransportType = 0
- V32ModemTransportType = 0
- V34ModemTransportType = 0
- BellModemTransportType = 0
- Additional configuration parameters:
  - CodersGroup
  - DJBufOptFactor
  - EnableSilenceCompression
  - EnableEchoCanceller

Note: This mode can be used for fax, but is not recommended for modem transmission. Instead, use the modes Bypass (see "Fax/Modem Bypass Mode" on page 250) or Transparent with Events (see "Fax / Modem Transparent with Events Mode" on page 252) for modem.

8.2.6.2.8 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

Relevant parameters:

- IsFaxUsed = 0 or 3
- FaxTransportType = 2
- FaxModemNTEMode = 1
- VxxModemTransportType = 2

8.2.6.3 V.152 Support

The device supports the ITU-T recommendation V.152 (Procedures for Supporting Voice-Band Data over IP Networks). Voice-band data (VBD) is the transport of modem, facsimile, and text telephony signals over a voice channel of a packet network with a codec appropriate for such signals.

For V.152 capability, the device supports T.38 as well as VBD codecs (i.e., G.711 A-law and G.711 µ-law). The selection of capabilities is performed using the coders table (see "Configuring Coders" on page 118).

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.

```
v=0
o=-  0 0 IN IPV4 <IPAdressA>
s=-
t=0 0
p=+1
c=IN IP4  <IPAddressA
m=audio <udpPort A> RTP/AVP 18 0
a=ptime:10
a=rtpmap:96 PCMU/8000
a=gpmd: 96 vbd=yes
```

In the example above, V.152 implementation is supported (using the dynamic payload type 96 and G.711 u-law as the VBD codec) as well as the voice codecs G.711 µ-law and G.729.

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.

8.2.6.4 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.

This feature is enabled using the T38FaxSessionImmediateStart parameter. The No-Op packets are enabled using the NoOpEnable and NoOpInterval parameters.

8.2.7 Working with Supplementary Services

The device supports the following supplementary services:

- Call Hold and Retrieve (see "Call Hold and Retrieve" on page 255)
- Call Pickup (see Call Pickup on page 257)
- Consultation (see Consultation Feature on page 257)
- Call Transfer (see "Call Transfer" on page 258)
- Call Forward (see "Call Forward" on page 259)
- Call Waiting (see Call Waiting on page 261)
- Message Waiting Indication (see "Message Waiting Indication" on page 262)
- Caller ID (see Caller ID on page 262)
- Three-way conferencing (see Three-Way Conferencing on page 265)
- Multilevel Precedence and Preemption (see "Multilevel Precedence and Preemption" on page 266)

To activate these supplementary services, enable each service's corresponding parameter using the Web interface or ini file.

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.

8.2.7.1 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.

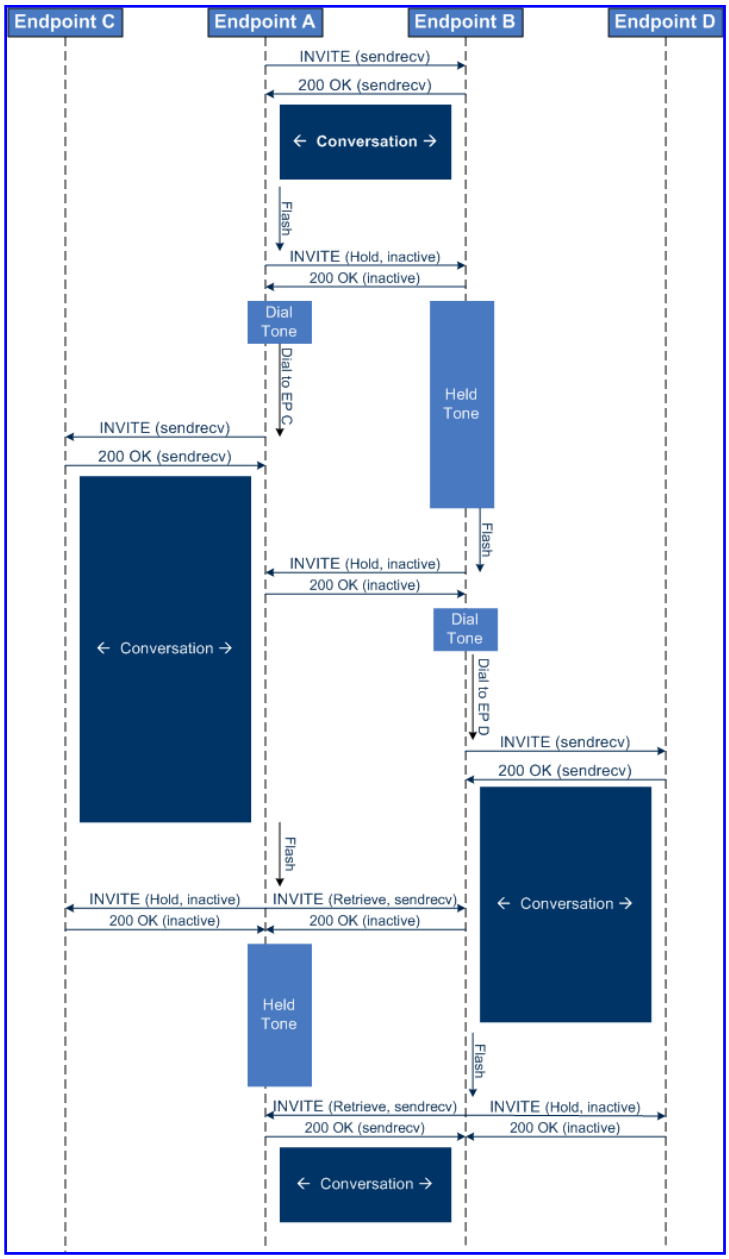
Receiving Hold/Retrieve:

- 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 8-15: 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).

8.2.7.2 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 Hunt Group ID.

8.2.7.3 Consultation Feature

The device's Consultation feature allows you to place one number on hold and consult privately with another party.

- The Consultation feature is relevant only for the holding 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.

8.2.7.4 Call Transfer

The device supports the following call transfer types:

- Consultation Transfer (see "Consultation Call Transfer" on page 258)
- Blind Transfer (see "Blind Call Transfer" on page 258)

Notes:

- Call transfer is initiated by sending REFER with REPLACES.
- The device can receive and act upon receiving REFER with or without REPLACES.
- The device can receive and act upon receiving INVITE with REPLACES, in which case the old call is replaced by the new one.
- The INVITE with REPLACES can be used to implement Directed Call Pickup.

8.2.7.4.1 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.

8.2.7.4.2 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 speaking to C. The result of the transfer is a call between B and C (similar to consultation transfer, but skipping the consultation stage).

8.2.7.5 Call Forward

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 157) or *ini* file to activate one of the call forward modes. These modes are configurable per endpoint.

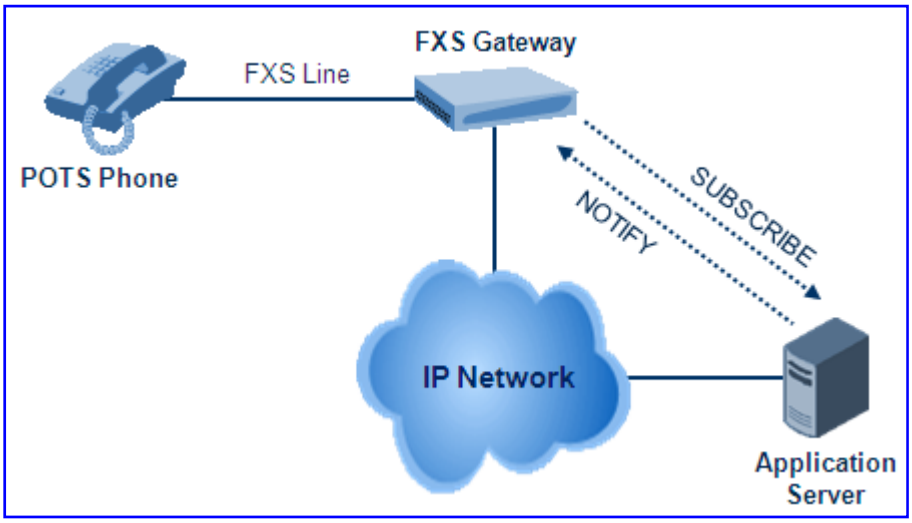
Notes:

- 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.

8.2.7.5.1 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 if 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 8-16: 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
- NRTRetrySubscriptionTime
- CallForwardRingToneID

8.2.7.5.2 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 cancelled. 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/simservs+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.

For cancelling 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/simservs+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

8.2.7.6 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 parameter FirstCallWaitingToneID in SIP Configuration Parameters).
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.

8.2.7.7 Message Waiting Indication

The device supports Message Waiting Indication (MWI) according to IETF Internet-Draft draft-ietf-sipping-mwi-04, including SUBSCRIBE (to MWI server).

Note: For a detailed description on IP voice mail configuration, refer to the *IP Voice Mail CPE Configuration Guide*.

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 (refer to the Product Reference Manual). 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).

To configure MWI, use the following parameters:

- EnableMWI
- MWIServerIP
- MWIAnalogLamp
- MWIDisplay
- StutterToneDuration
- EnableMWISubscription
- MWIExpirationTime
- SubscribeRetryTime
- SubscriptionMode
- CallerIDType (determines the standard for detection of MWI signals)
- ETSIVMWITypeOneStandard
- BellcoreVMWITypeOneStandard
- VoiceMailInterface
- EnableVMURI

8.2.7.8 Caller ID

This section discusses the device's Caller ID support.

8.2.7.8.1 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.
- AnalogCallerIDTimimgMode: 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.

8.2.7.8.2 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**.

8.2.7.8.3 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: "David" <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

In addition, the caller ID (and presentation) can 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.

8.2.7.9 Three-Way Conferencing

The device supports three-way conference calls. These conference calls can also occur simultaneously.

The following example demonstrates three-way conferencing. This example assumes that a telephone "A" connected to the device wants to establish a three-way conference call with two remote IP phones "B" and "C":

1. User A has an ongoing call with IP phone B.
2. User A places IP phone B on hold (by pressing the telephone's flash hook button, defined by the parameter HookFlashCode).
3. User A hears a dial tone, and then makes a call to IP phone C.
4. IP phone C answers the call.
5. User A can now establish a three-way conference call (between A, B and C) by pressing the flash-hook button, defined by the parameter ConferenceCode (e.g., regular flash-hook button or "*1").

Notes:

- 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 interfaces.

The device supports the following conference modes (configured by the parameter 3WayConferenceMode):

- **Conferencing controlled 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 controlled 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, whereby 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 device utilizes resources from idle ports to establish the conference call. The number of simultaneous on-board conferences can be limited using the parameter MaxInBoardConferenceCalls. In addition, you can designate ports that can't be used as a resource for conference calls initiated by other ports, using the parameter 3WayConfNoneAllocateablePorts. Ports that are not configured with this parameter (and that are idle) are used by the device as a resource for establishing these type of conference calls. For this mode, the 3WayConferenceMode parameter is set to 2.

To enable three-way conferencing, the following parameters need to be configured:

- Enable3WayConference
- ConferenceCode = '!' (default, which is the hook flash button)
- HookFlashCode
- 3WayConferenceMode (conference mode)
- MaxInBoardConferenceCalls (if on-board conferencing)
- 3WayConfNoneAllocateablePorts (if on-board conferencing)
- FlashKeysSequenceStyle = 1 or 2 (makes a three-way call conference using the Flash button + 3)

Note: For local, on-board three-way conferencing on MP-112, in addition to configuring the previously mentioned parameters, the following parameter settings must be included:

```
EnableIPMediaChannels = 1
[ IPMediaChannels ]
FORMAT IPMediaChannels_Index = IPMediaChannels_ModuleID, IPMediaChannels_DSPChannelsReserved;
IPMediaChannels 0 = 1, 2;
[ \IPMediaChannels ]
```

8.2.7.10 Multilevel Precedence and Preemption

The device's Multilevel Precedence and Preemption (MLPP) service can be enabled using the CallPriorityMode parameter. MLPP is a call priority scheme, which does the following:

- Assigns a precedence level (priority level of call) 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 go 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.

The Resource Priority value in the Resource-Priority SIP header can be any on of those listed in the table below. For each MLPP call priority level, the Multiple Differentiated Services Code Points (DSCP) can be set to a value from 0 to 63.

Table 8-3: 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

MLPP Precedence Level	Precedence Level in Resource-Priority SIP Header	DSCP Configuration Parameter
8	flash-override	MLPPFlashOverRTPDSCP
9 (highest)	flash-override-override	MLPPFlashOverOverRTPDSCP

- **Precedence Ring Tone:** You can assign a ring tone (in the CPT file) that is played when a Precedence call is received from the IP side. This is configured by the parameter PrecedenceRingingType.
- Emergency Telecommunications Services calls (e.g., E911): ETS calls can be configured to be regarded as having a higher priority than any MLPP call (default), using the E911MLPPBehavior parameter.
- **MLPP Preemption Events in SIP Reason Header:** The device sends the SIP Reason header (as defined in RFC 4411) to indicate the reason a preemption event occurred and the type of preemption event. The device sends a SIP BYE or CANCEL request, or 480, 486, 488 responses (as appropriate) with a Reason header whose Reason-params can includes 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"
  - Reason: preemption; cause=5; text="Network Preemption"

  Cause=4: The Reason cause code "Non-IP Preemption" 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.

  Cause=5: The Reason cause code "Network Preemption" 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

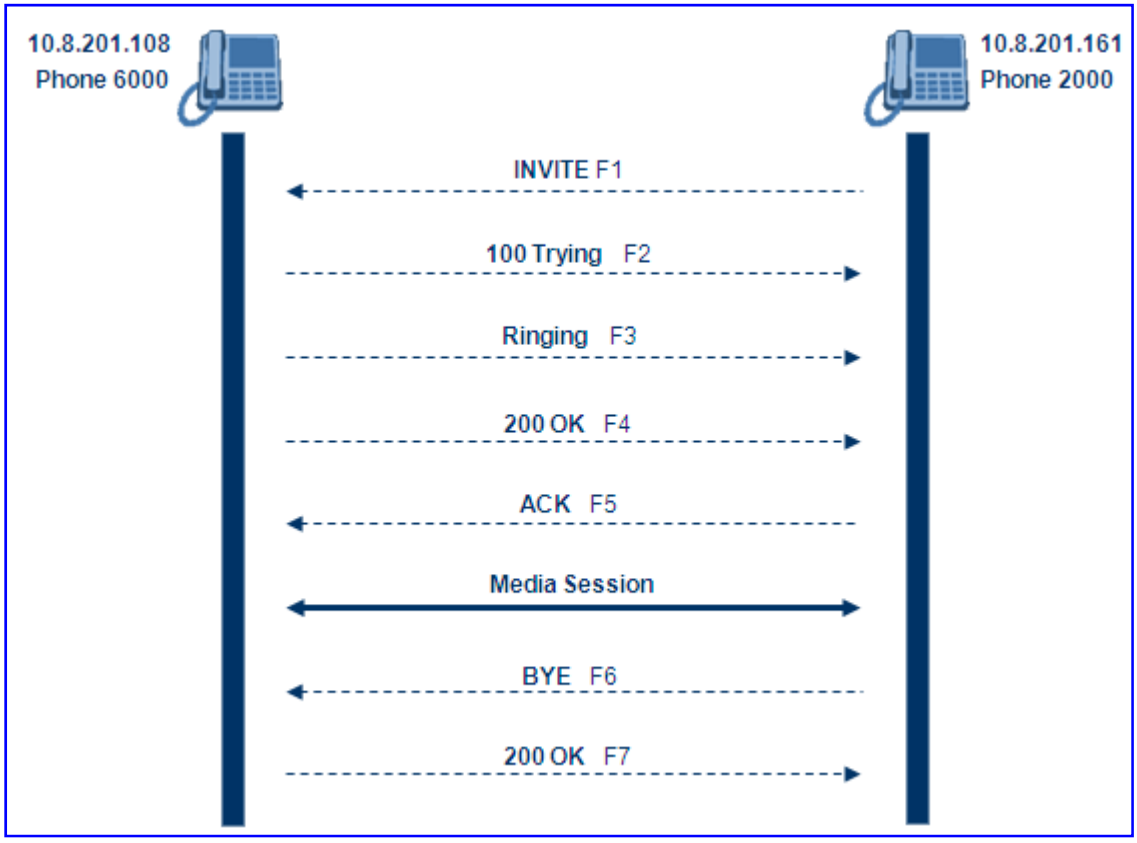
For a complete list of the MLPP parameters, see "MLPP Parameters" on page 454.

8.2.8 SIP Call Routing Examples

8.2.8.1 SIP Call Flow Example

The SIP call flow (shown in the following figure), describes SIP messages exchanged between two devices during a basic call. In this call flow example, device (10.8.201.158) with phone number '6000' dials device (10.8.201.161) with phone number '2000'.

Figure 8-17: SIP Call Flow



- **F1 INVITE (10.8.201.108 >> 10.8.201.161):**

```
INVITE sip:2000@10.8.201.161;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
CSeq: 18153 INVITE
Contact: <sip:8000@10.8.201.108;user=phone>
User-Agent: Audiocodes-Sip-Gateway/MediaPack/v.6.00.010.006
Supported: 100rel,em
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,
NOTIFY,PRACK,REFER,INFO
Content-Type: application/sdp
Content-Length: 208
v=0
o=AudiocodesGW 18132 74003 IN IP4 10.8.201.108
s=Phone-Call
c=IN IP4 10.8.201.108
t=0 0
m=audio 4000 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

- **F2 TRYING (10.8.201.161 >> 10.8.201.108):**

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
Server: Audiocodes-Sip-Gateway/MediaPack/v.6.00.010.006
CSeq: 18153 INVITE
Content-Length: 0
```

- **F3 RINGING 180 (10.8.201.161 >> 10.8.201.108):**

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>;tag=1c7345
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
Server: Audiocodes-Sip-Gateway/MediaPack/v.6.00.010.006
CSeq: 18153 INVITE
Supported: 100rel,em
Content-Length: 0
```

Note: Phone '2000' answers the call and then sends a 200 OK message to device 10.8.201.108.

- **F4 200 OK (10.8.201.161 >> 10.8.201.108):**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacsiJkDGd
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>;tag=1c7345
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
CSeq: 18153 INVITE
Contact: <sip:2000@10.8.201.161;user=phone>
Server: Audiocodes-Sip-Gateway/MediaPack/v.6.00.010.006
Supported: 100rel,em
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,
NOTIFY,PRACK,REFER,INFO
Content-Type: application/sdp
Content-Length: 206
v=0
o=AudiocodesGW 30221 87035 IN IP4 10.8.201.161
s=Phone-Call
c=IN IP4 10.8.201.10
t=0 0
m=audio 7210 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=ptime:20
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
```

- **F5 ACK (10.8.201.108 >> 10.8.201.10):**

```
ACK sip:2000@10.8.201.161;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacZYpJWxZ
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>;tag=1c7345
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
User-Agent: Audiocodes-Sip-Gateway/MediaPack/v.6.00.010.006
CSeq: 18153 ACK
Supported: 100rel,em
Content-Length: 0
```

Note: Phone '6000' goes on-hook and device 10.8.201.108 sends a BYE to device 10.8.201.161. A voice path is established.

- **F6 BYE (10.8.201.108 >> 10.8.201.10):**

```
BYE sip:2000@10.8.201.161;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacRKCVBud
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>;tag=1c7345
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
User-Agent: Audiocodes-Sip-Gateway/MediaPack/v.6.00.010.006
CSeq: 18154 BYE
Supported: 100rel,em
Content-Length: 0
```

- **F7 OK 200 (10.8.201.10 >> 10.8.201.108):**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.201.108;branch=z9hG4bKacRKCVBud
From: <sip:6000@10.8.201.108>;tag=1c5354
To: <sip:2000@10.8.201.161>;tag=1c7345
Call-ID: 534366556655skKw-6000--2000@10.8.201.108
Server: Audiocodes-Sip-Gateway/MediaPack/v.6.00.010.006
CSeq: 18154 BYE
Supported: 100rel,em
Content-Length: 0
```

8.2.8.2 SIP 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 401 Unauthorized response to challenge authentication containing a WWW-Authenticate header, and expect the re-INVITE to contain an Authorization header.

The following example describes 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: Audiocodes-Sip-Gateway/MediaPack/v.6.00.010.006
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 2001 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 (according to RFC this part is called A1) **'122:audiocodes.com:AudioCodes'.**
   - The MD5 algorithm is run on this equation and stored for future usage.
   - The result is 'a8f17d4b41ab8dab6c95d3c14e34a9e1'.
5. Next, the par called A2 needs to be evaluated:
   - The method type is 'REGISTER'.
   - Using SIP protocol 'sip'.
   - Proxy IP from *ini* file is '10.2.2.222'.
   - The equation to be evaluated is **'REGISTER:sip:10.2.2.222'.**
   - The MD5 algorithm is run on this equation and stored for future usage.
   - The result is 'a9a031cfddcb10d91c8e7b4926086f7e'.
6. Final stage:
   - The A1 result: The nonce from the proxy response is '11432d6bce58ddf02e3b5e1c77c010d2'.
   - The 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/MediaPack/v.6.00.010.006
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 closing the REGISTER 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 2001 09:34:42 GMT
Server: Columbia-SIP-Server/1.17
Content-Length: 0
Contact: <sip:122@10.1.1.200>; expires="Thu, 26 Jul 2001 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 2001 10:34:42 GMT
```

8.2.8.3 Establishing a Call between Two Devices

This section provides an example on configuring two AudioCodes' devices with FXS interfaces for establishing call communication. After configuration, you can make calls between telephones connected to the same device and between the two devices.

This example assumes the following:

- The IP address of the first device is 10.2.37.10 and its endpoint numbers are 101 to 104.
- The IP address of the second device is 10.2.37.20 and its endpoint numbers are 201 to 204.
- A SIP Proxy is not used. Internal call routing is performed using the device's 'Tel to IP Routing'.

➢ **To configure the two devices for call communication:**

1. For the *first* device (10.2.37.10), in the 'Endpoint Phone Number Table' page (see Configuring Endpoint Phone Numbers on page 124), assign the phone numbers 101 to 104 to the device's endpoints.

Figure 8-18: Assigning Phone Numbers to Device 10.2.37.10

	Channel(s)	Phone Number	Hunt Group ID
1	1-4	101	

2. For the *second* device (10.2.37.20), in the 'Endpoint Phone Number Table' page, assign the phone numbers 201 to 204 to the device's endpoints.

Figure 8-19: Assigning Phone Numbers to Device 10.2.37.20

	Channel(s)	Phone Number	Hunt Group ID
1	1-4	201	

3. Configure the following settings for *both* devices:

   In the 'Tel to IP Routing' page (see "Configuring Tel to IP Routing" on page 138), add the following routing rules:

   a. In the first row, enter 10 for the destination phone prefix and enter 10.2.37.10 for the destination IP address (i.e., IP address of the first device).
   b. In the second row, enter 20 for the destination phone prefix and 10.2.37.20 for the destination IP address (i.e., IP address of the second device).

   These settings enable the routing (from both devices) of outgoing Tel-to-IP calls that start with 10 to the first device and calls that start with 20 to the second device.

Figure 8-20: Routing Calls Between Devices

	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address
1	10	*		10.2.37.10
2	20	*		10.2.37.20

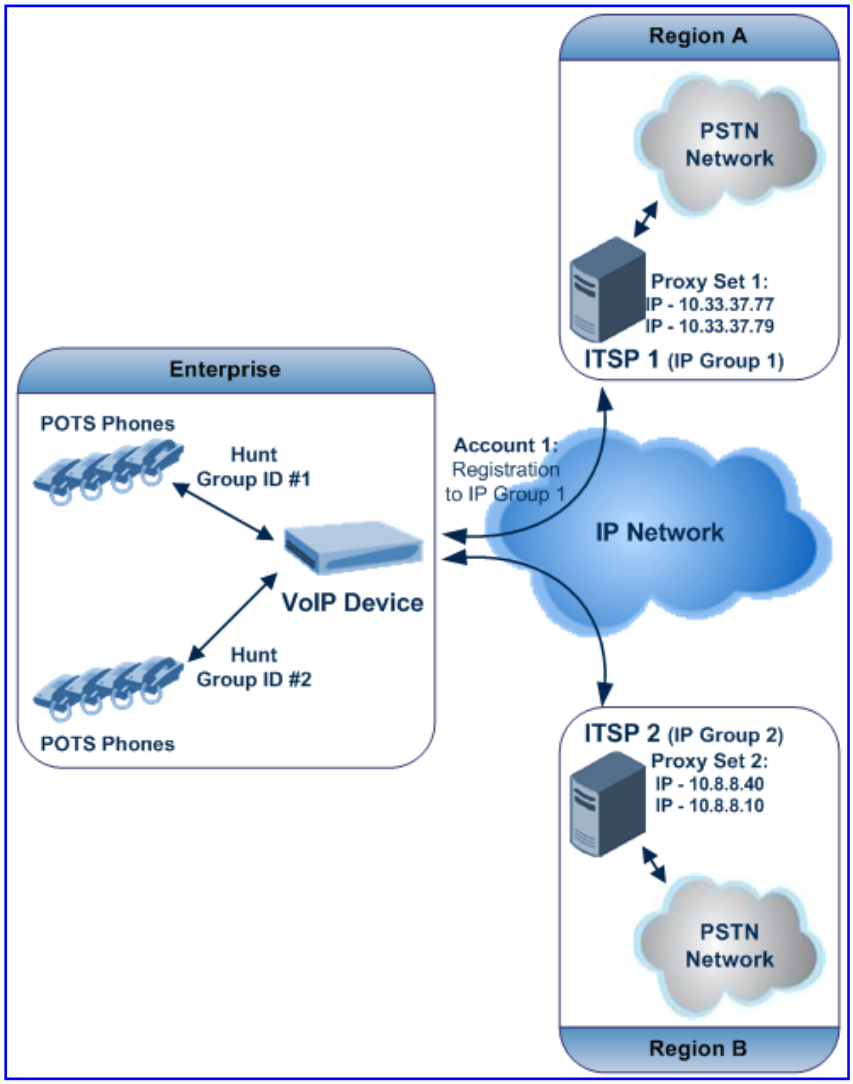
4. Make a call. Pick up the phone connected to port #1 of the first device and dial 102 (to the phone connected to port #2 of the same device). Listen for progress tones at the calling phone and for the ringing tone at the called phone. Answer the called phone, speak into the calling phone, and check the voice quality. Dial 201 from the phone connected to port #1 of the first device; the phone connected to port #1 of the second device rings. Answer the call and check the voice quality.

8.2.8.4 SIP Trunking between Enterprise and ITSPs

By implementing the device's enhanced and flexible routing capabilities, you can "design" complex routing schemes. This section provides an example of an elaborate routing scheme for SIP trunking between an Enterprise and two Internet Telephony Service Providers (ITSP), using AudioCodes device.

Scenario: In this example, an Enterprise has deployed the device with eight FXS interfaces. The first four phones operate with ITSP 1 (using UDP), while the next four phones (channels 5-8) operate with ITSP 2 (using TCP). ITSP 1 requires single registration (i.e., one registration for all four phones), while ITSP 2 requires registration per phone. Each ITSP implements two servers for redundancy and load balancing. The figure below illustrates this example setup:

Figure 8-21: Routing Between ITSPs and Enterprise (Example)



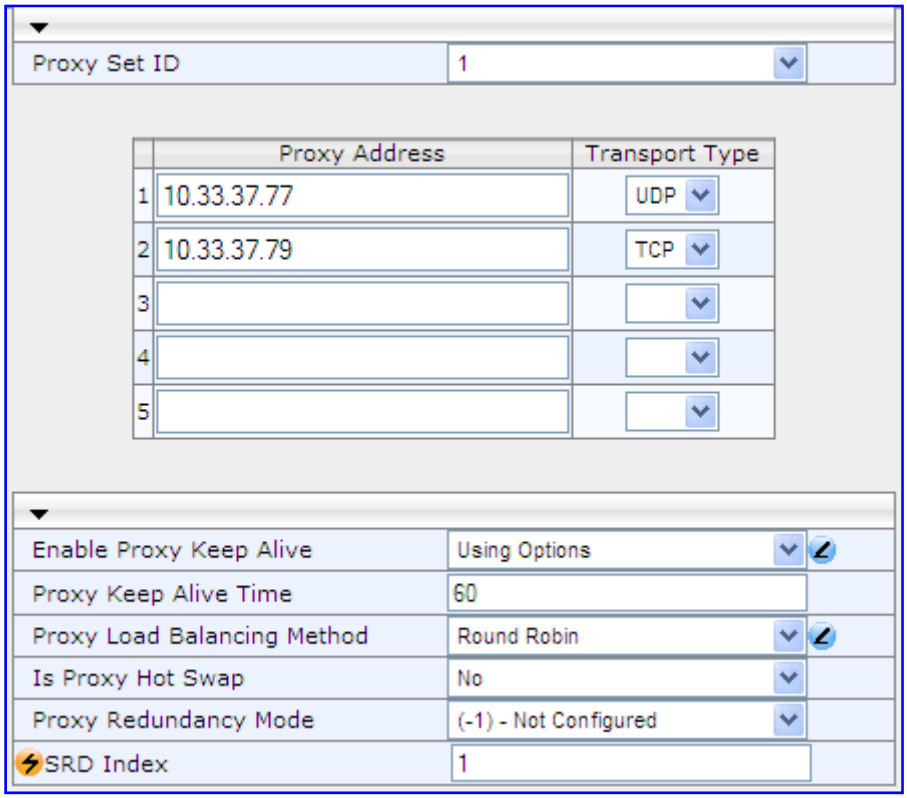
➢ **To configure call routing between an Enterprise and two ITSPs:**

1. Enable the device to register to a Proxy/Registrar server using the parameter IsRegisterNeeded.

2. In the 'Proxy Sets Table' page (see "Configuring Proxy Sets Table" on page 106), configure two Proxy Sets and for each, enable Proxy Keep-Alive (using SIP OPTIONS) and 'round robin' load-balancing method:
   - Proxy Set **#1** includes two IP addresses of the first ITSP (**ITSP 1**) - 10.33.37.77 and 10.33.37.79 - and using UDP.
   - Proxy Set **#2** includes two IP addresses of the second ITSP (**ITSP 2**) - 10.8.8.40 and 10.8.8.10 - and using TCP.

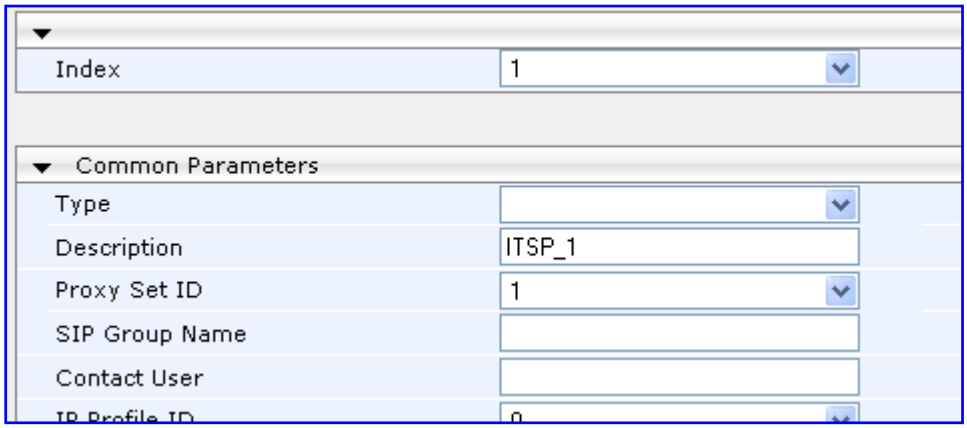
   The figure below displays the configuration of Proxy Set ID #1. Perform similar configuration for Proxy Set ID #2, but using different IP addresses.

Figure 8-22: Configuring Proxy Set ID #1 in the Proxy Sets Table Page



3. In the 'IP Group Table' page (see "Configuring IP Groups" on page 103), configure the two IP Groups #1 and #2. Assign Proxy Sets #1 and #2 to IP Groups #1 and #2 respectively.

Figure 8-23: Configuring IP Groups #1 and #2 in the IP Group Table Page



4. In the 'Endpoint Phone Number Table' page, configure Hunt Group ID #1 for channels 1-4, and Hunt Group ID #2 for channels 5-8.

Figure 8-24: Assigning Channels to Hunt Groups

	Channel(s)	Phone Number	Hunt Group ID	Tel Profile ID
1	1-4	401	1	
2	5-8	405	2	

5. In the 'Hunt Group Settings' page, configure 'Per Account' registration for Hunt Group ID #1 (without serving IP Group) and associate it with IP Group #1; Configure 'Per Endpoint' registration for Hunt Group ID #2 and associated it with IP Group #2.

Figure 8-25: Configuring Registration Mode for Hunt Groups and Assigning to IP Group

	Hunt Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	1	Cyclic Ascending	Per Account	1		
2	2	Cyclic Ascending	Per Endpoint	2		

6. In the 'Authentication' page, for channels 5-8 (i.e., Hunt Group ID #2), define for each channel the registration (authentication) user name and password.

Figure 8-26: Configuring Username and Password for Channels 5-8 in Authentication Page

Gateway Port	User Name	Password
Port 1 FXS		
Port 2 FXS		
Port 3 FXS		
Port 4 FXS		
Port 5 FXS	user1	1111
Port 6 FXS	user2	2222
Port 7 FXS	user3	3333
Port 8 FXS	user4	4444

7. In the 'Account Table' page, configure a single Account for Hunt Group ID #1, including an authentication user name and password, and enable registration for this Account to ITSP 1 (i.e., Serving IP Group is 1).

Figure 8-27: Configuring Account for Registration to ITSP 1

Index	ServedTrunkGroup	ServingIPGroup	Username	Password	HostName	Register
2	1	1	ITSP1user	1234	ITSP1	1

8. In the 'IP to Hunt Group Routing Table' page, configure that INVITEs with "ITSP1" as the hostname in the From URI are routed to Hunt Group #1, and INVITEs with "ITSP2" as the hostname in the From URI are routed to Hunt Group #2. In addition, configure calls received from ITSP1 as associated with IP Group #1.

Figure 8-28: Configuring ITSP-to-Hunt Group Routing

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	->	Hunt Group ID	IP Profile ID	Source IPGroup ID
1		ITSP1	*	*			1		1
2		ITSP2	*	*			2		

9. In the 'Tel to IP Routing' page, configure Tel-to-IP routing rules for calls from Hunt Group #1 to IP Group #1, and from Hunt Group #2 to IP Group #2.

Figure 8-29: Configuring Hunt Group to ITSP Routing

Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	->	Dest. IP Address	Port	Transport Type	Dest. IPGroup ID
1	*	*				Not Configured	1
2	*	*				Not Configured	2

8.2.9 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 parameter DisconnectOnBusyTone is set to 0, the FXO device ignores the detection of Busy/Reorder tones and doesn't release the call.
- For all other FXS/FXO release types (caused when there are no free channels in the specific Hunt Group), or when an appropriate rule for routing the call to a Hunt Group doesn't exist, or if the phone number isn't found), the device sends a SIP response (to IP) according to the parameter DefaultReleaseCause. 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.

8.2.10 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 as well as the number of free (available) telephone channels
- **mediachs:** not applicable

Below is an example of the X-Resources:

```
X-Resources: telchs= 8/4;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 8 channels are available).

8.3 Stand-Alone Survivability (SAS) Application

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. In addition, typically these failures 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 Upgrade Key.
- Throughput 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.

8.3.1 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 a detailed description, see "SAS Outbound Mode" on page 280.
- **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 a detailed description, see "SAS Redundant Mode" on page 282.

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

8.3.1.1 SAS Outbound Mode

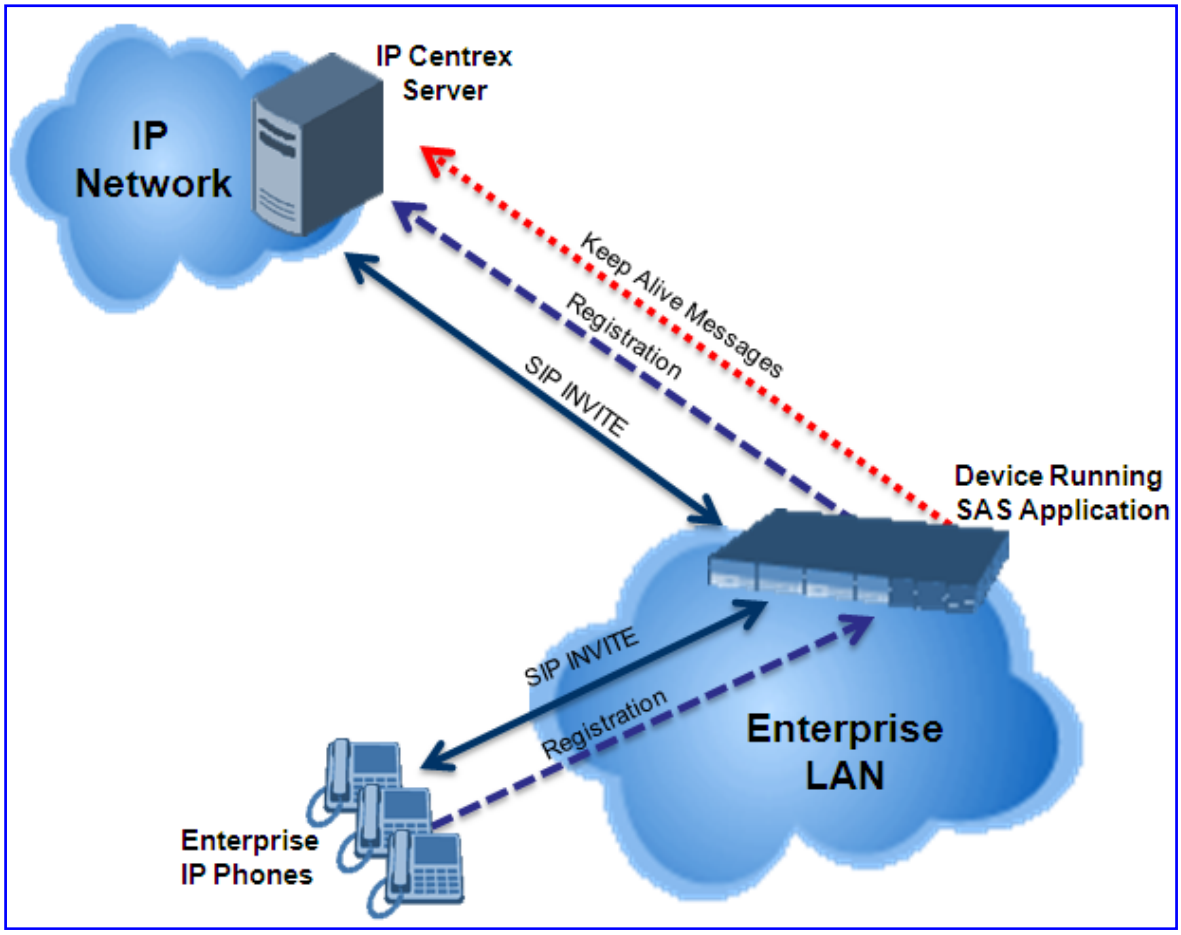
This section describes the SAS outbound mode, which includes the following states:

- Normal state (see "Normal State" on page 280)
- Emergency state (see "Emergency State" on page 281)

8.3.1.1.1 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. In addition, SAS 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 8-30: SAS Outbound Mode in Normal State (Example)



8.3.1.1.2 Emergency State

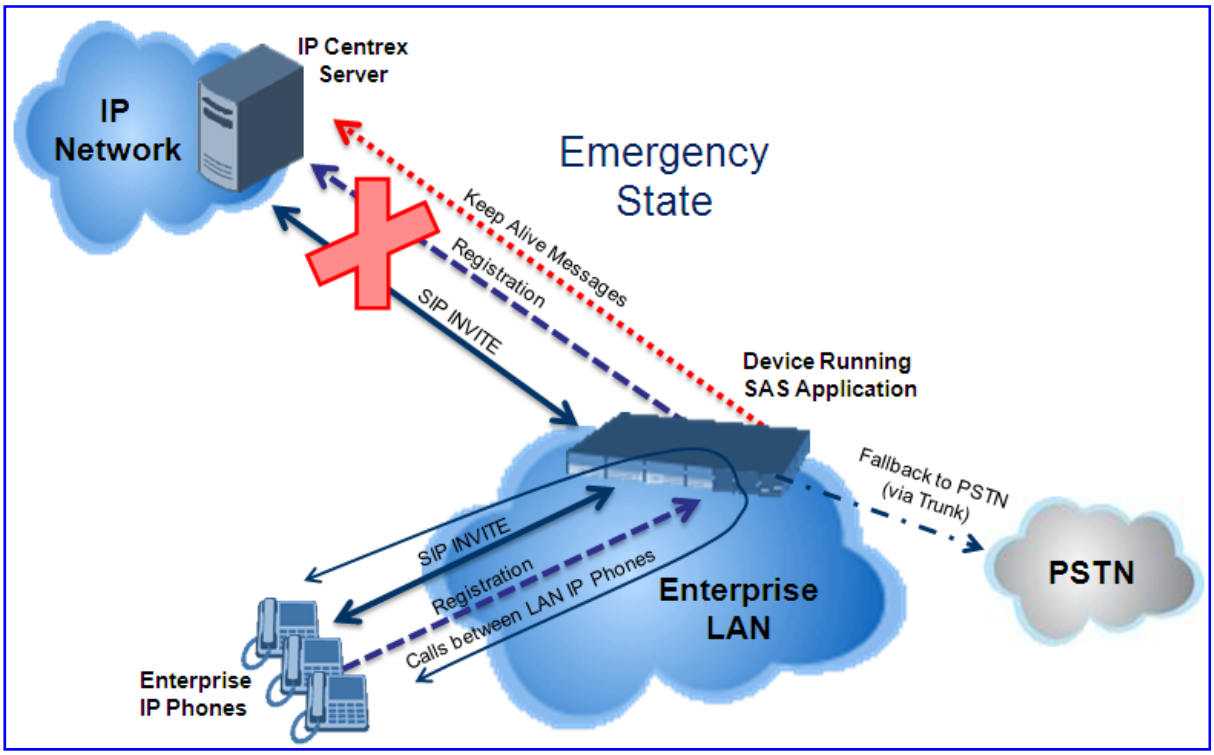
When a connection with the external proxy fails (detected by the device's keep-alive messages), the device enters SAS emergency state. The device serves as a proxy for the UAs, by handling internal call routing of the UAs (within the LAN enterprise).

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 286.

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

Figure 8-31: 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 283.

8.3.1.2 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).

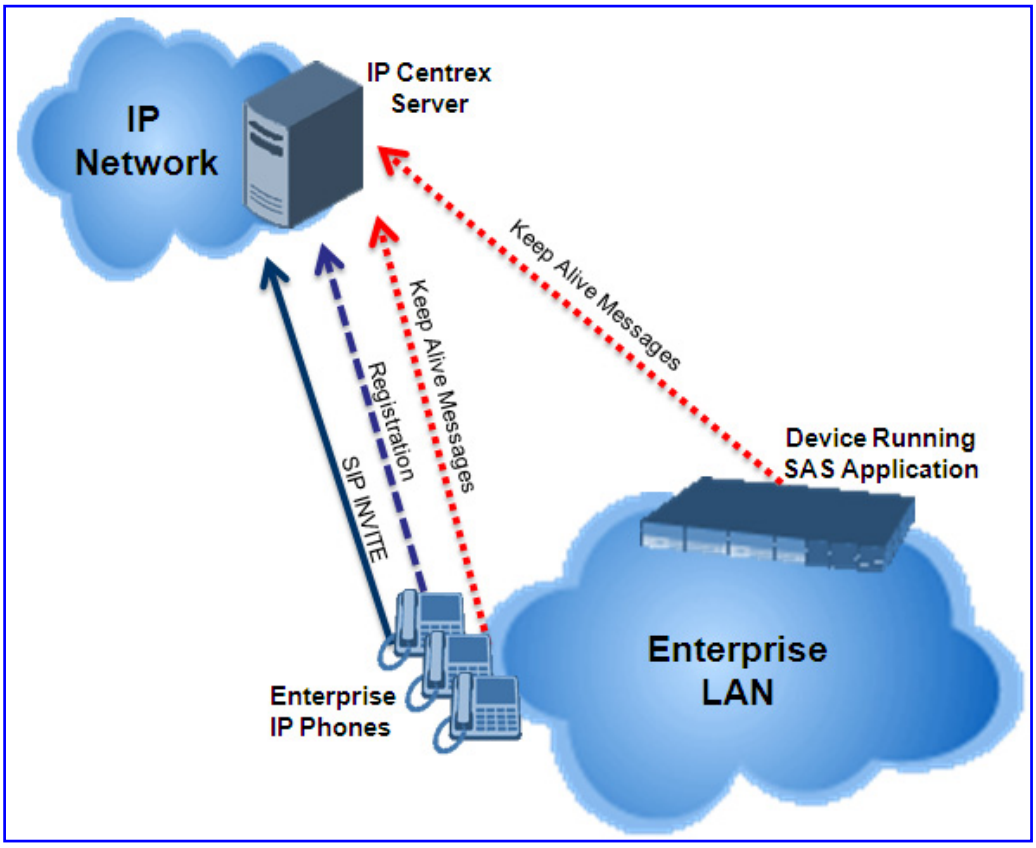
This mode is operational only during SAS in emergency state.

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.

8.3.1.2.1 Normal State

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

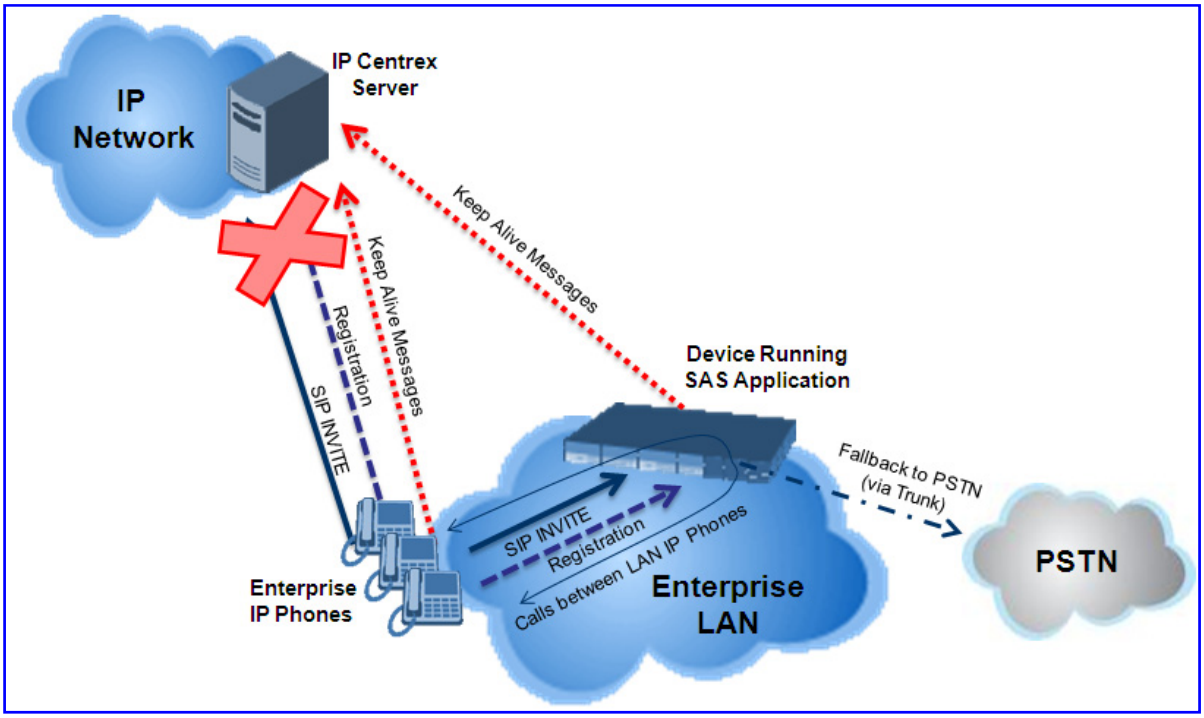
Figure 8-32: SAS Redundant Mode in Normal State (Example)



8.3.1.2.2 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 8-33: SAS Redundant Mode in Emergency State (Example)



8.3.1.2.3 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).

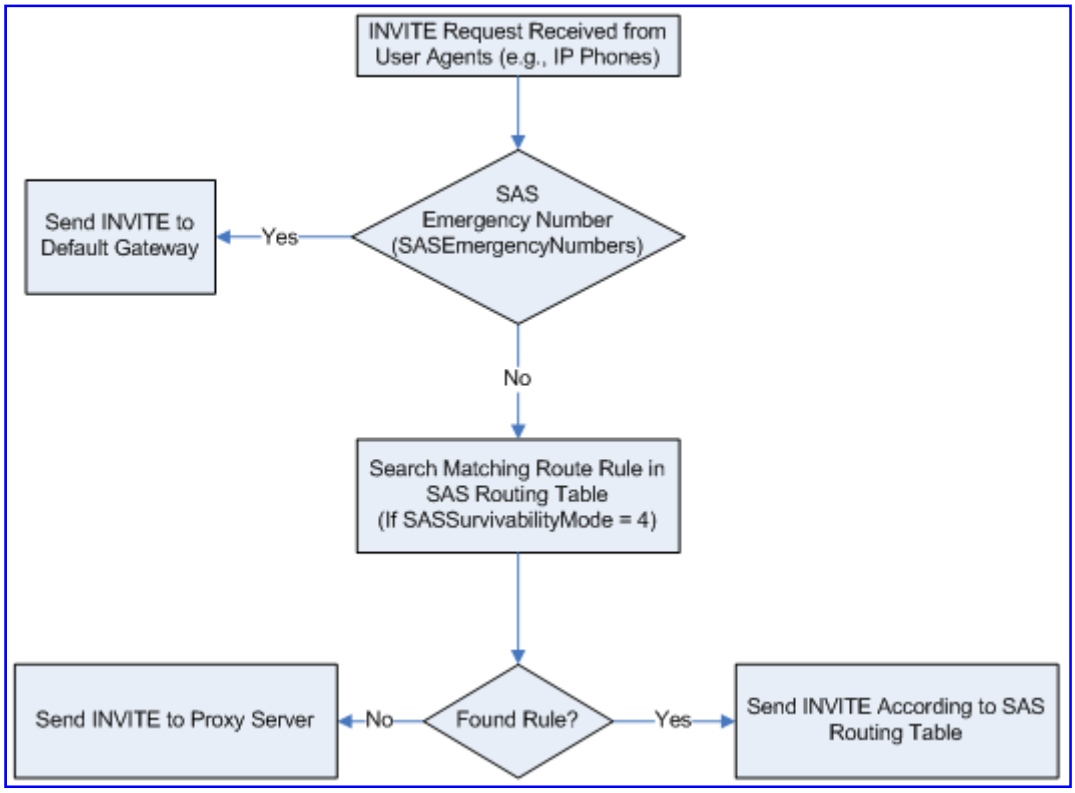
8.3.2 SAS Routing

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

8.3.2.1 SAS Routing in Normal State

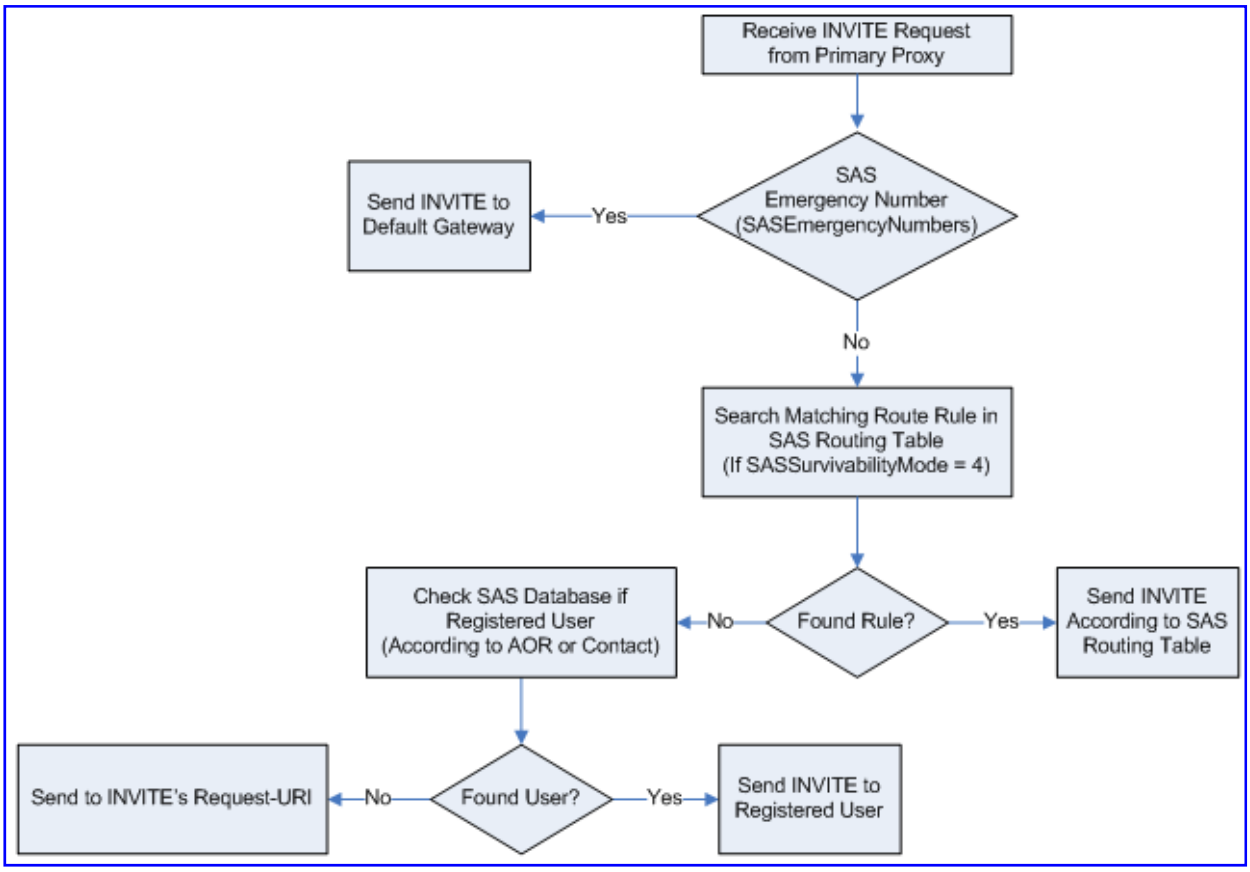
The flowchart below displays the routing logic for SAS in normal state for INVITE messages received from the UAs:

Figure 8-34: 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:

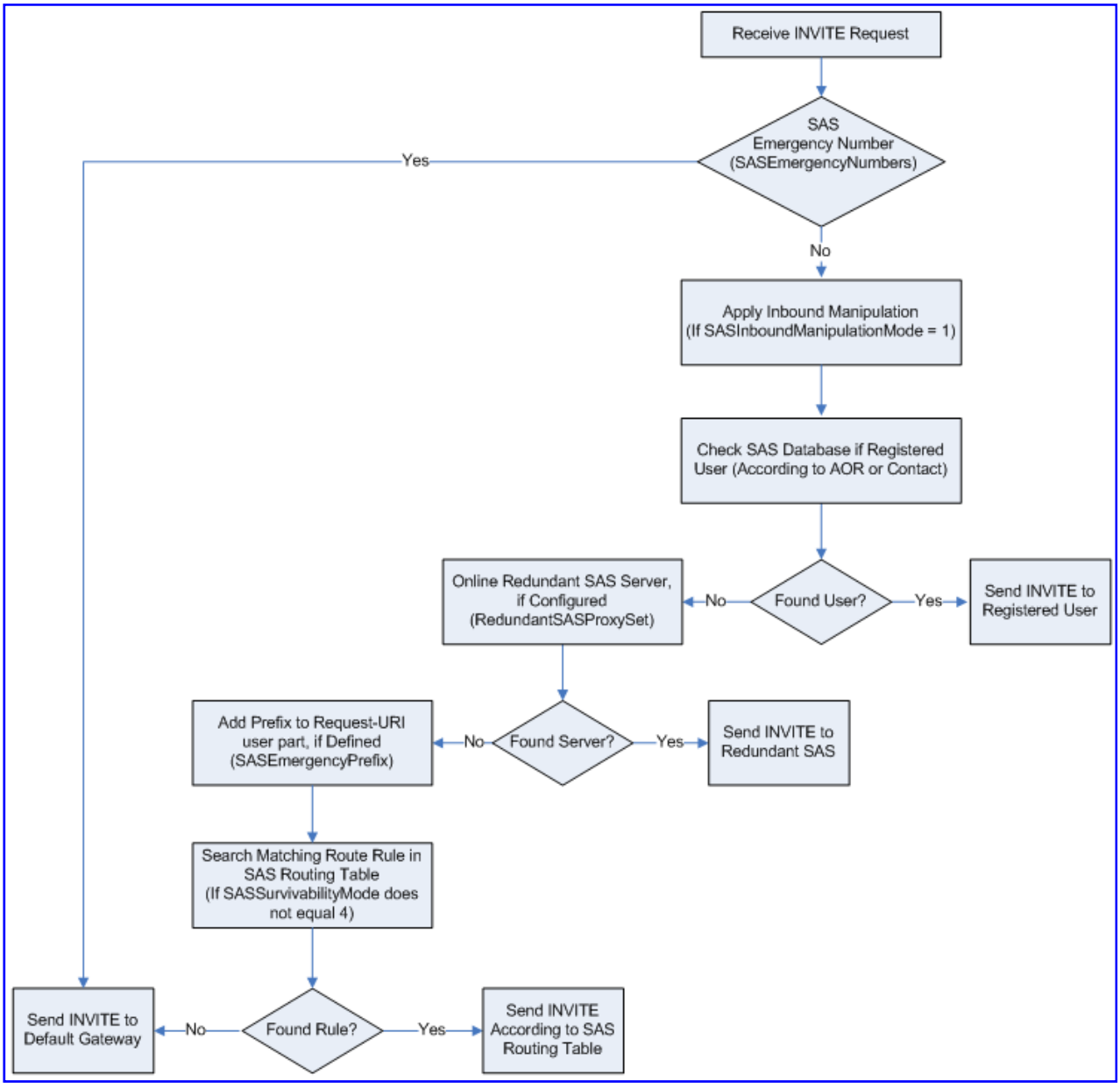
Figure 8-35: Flowchart of INVITE from Primary Proxy in SAS Normal State



8.3.2.2 SAS Routing in Emergency State

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

Figure 8-36: Flowchart for SAS Emergency State



8.3.3 SAS Configuration

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

The SAS configuration includes the following:

- General SAS configuration that is common to all SAS deployment types (see "General SAS Configuration" on page 287)
- SAS outbound mode (see "Configuring SAS Outbound Mode" on page 290)
- SAS redundant mode (see "Configuring SAS Redundant Mode" on page 291)
- Gateway and SAS applications deployed together (see "Configuring Gateway Application with SAS" on page 291)
- Optional, advanced SAS features (see "Advanced SAS Configuration" on page 295)

8.3.3.1 General SAS Configuration

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

8.3.3.1.1 Enabling the SAS Application

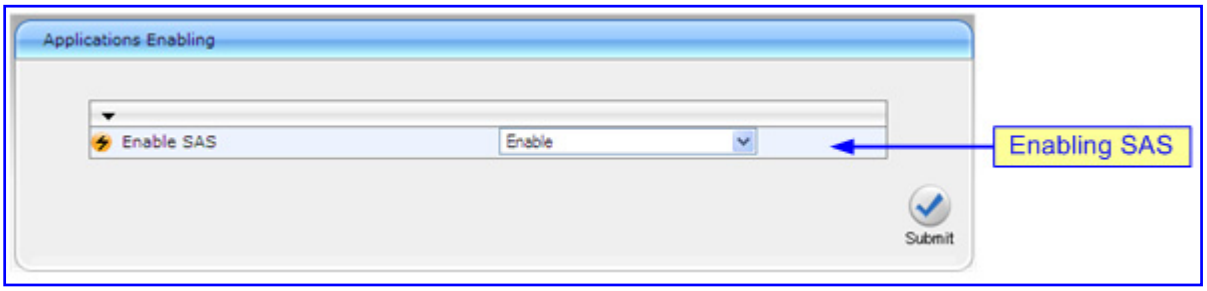
Before you can configure SAS, you need to enable the SAS application on the device. Once enabled, the device's Web interface provides the SAS pages for configuring SAS.

Note: The SAS application is available only if the device is installed with the SAS Software Upgrade 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 'Enable SAS' drop-down list, select 'Enable'.

Figure 8-37: Enabling the SAS Application



3. Click **Submit**.
4. Save the changes to the flash memory with a device reset; after the device resets, the SAS menu appears and you can now begin configuring the SAS application.

8.3.3.1.2 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:**

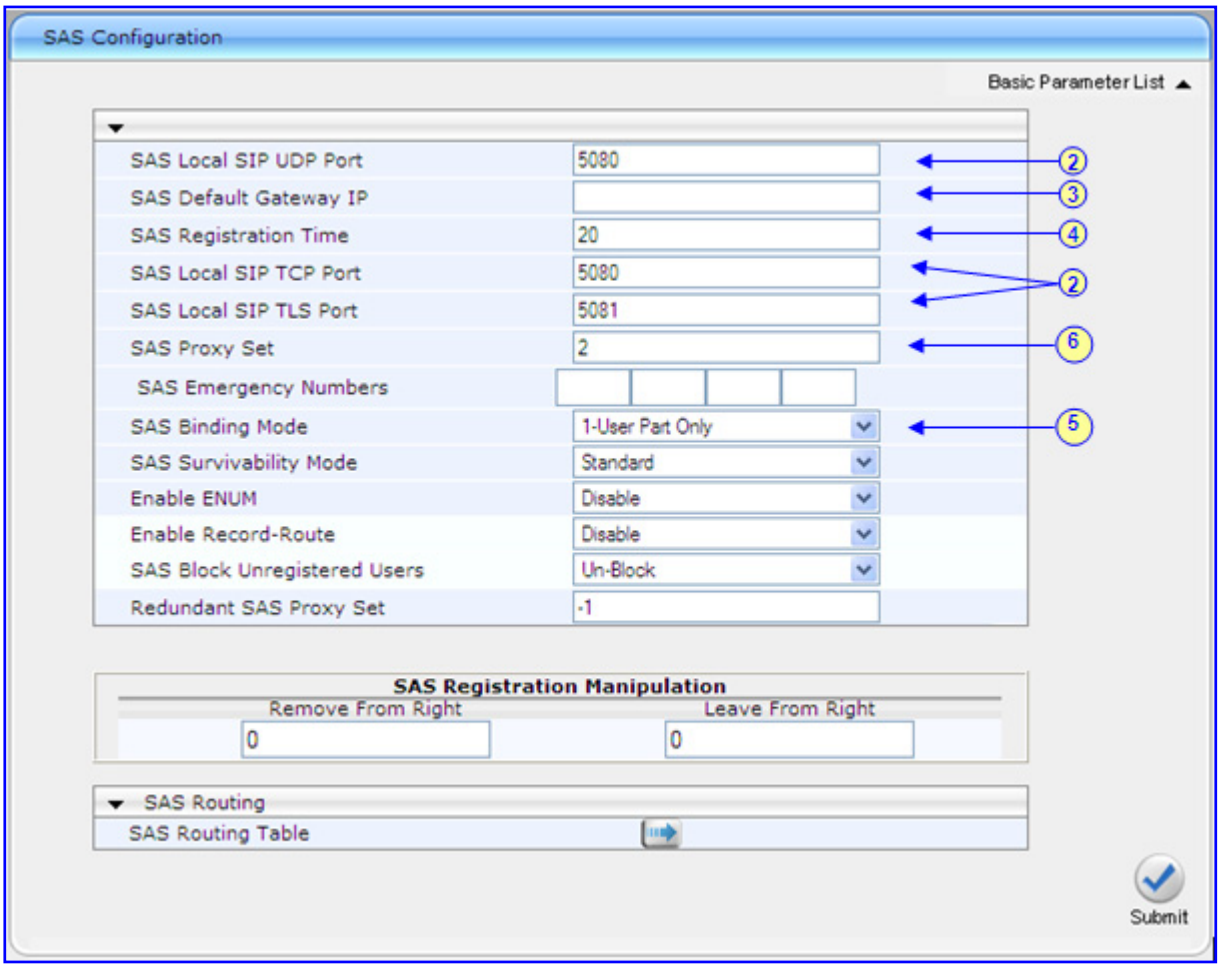
1. Open the 'SAS Configuration' page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. Define the port used for sending and receiving SAS messages. This can be any of the following port types:
   - UDP port - defined in the 'SAS Local SIP UDP Port' field
   - TCP port - 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 8-38: Configuring Common Settings



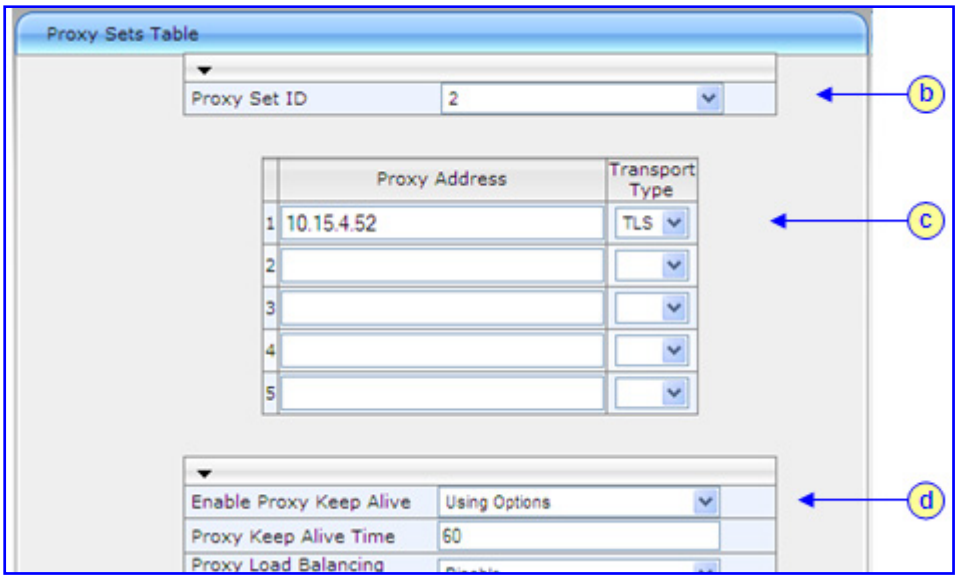
6. In the 'SAS Proxy Set' field, enter the Proxy Set used for SAS. The SAS Proxy Set must be defined only for the following SAS modes:
   - **Outbound mode:** In SAS normal state, SAS forwards REGISTER and INVITE messages received from the UAs to the proxy servers defined in this Proxy Set.
   - **Redundant 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 8-39: Defining UAs' Proxy Server



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

8.3.3.2 Configuring SAS Outbound Mode

This section describes how to configure the SAS outbound mode. These settings are in addition to the ones described in "Configuring Common SAS Parameters" on page 288.

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**.

8.3.3.3 Configuring SAS Redundant Mode

This section describes how to configure the SAS redundant mode. These settings are in addition to the ones described in "Configuring Common SAS Parameters" on page 288.

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**.

8.3.3.4 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.

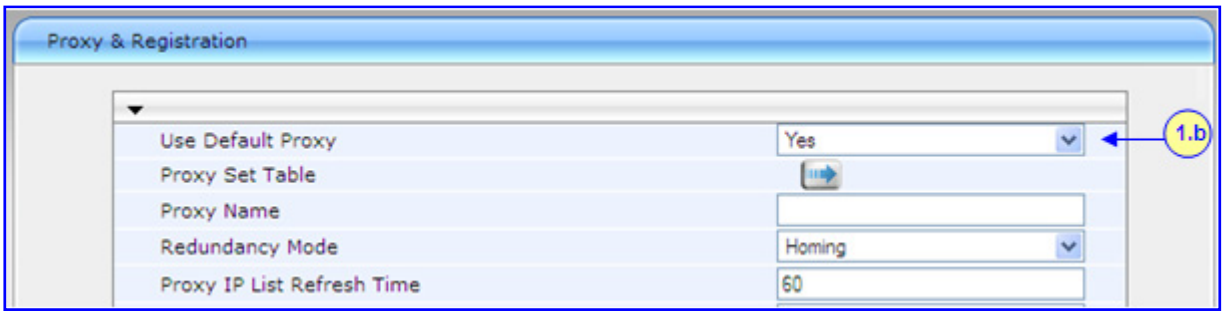
8.3.3.4.1 Gateway with SAS Outbound Mode

The procedure below describes how to configure the Gateway application with SAS outbound mode.

➢ **To configure Gateway application with SAS outbound mode:**

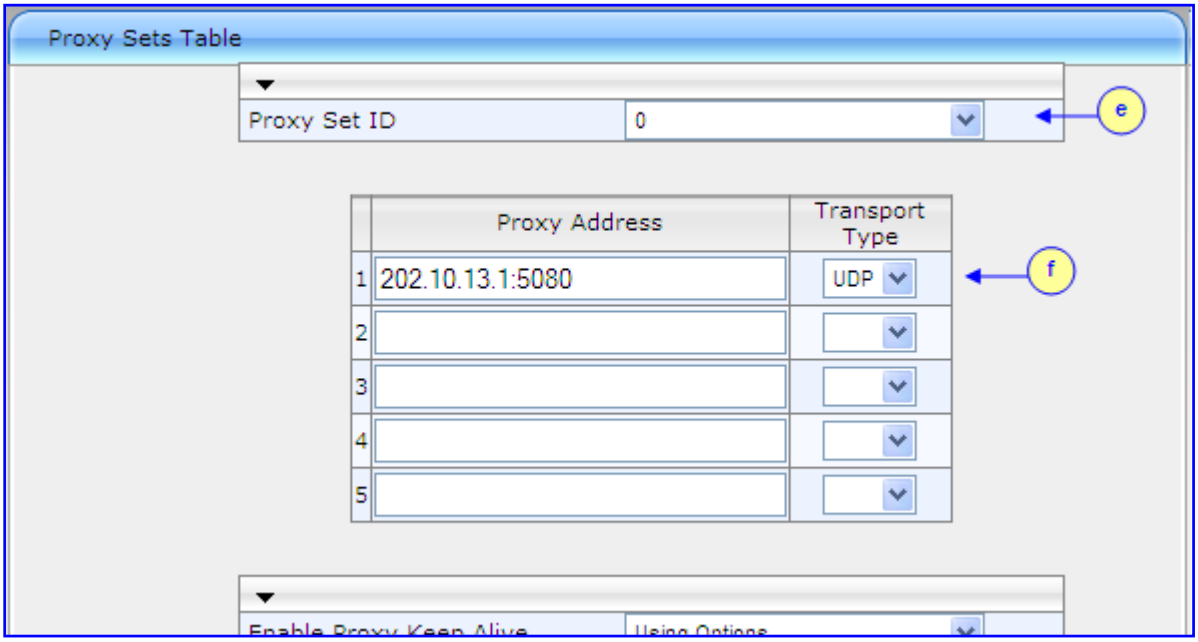
1. Define the proxy server address for the Gateway application:
   a. Open the 'Proxy & Registration' page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Proxy & Registration**).
   b. From the 'Use Default Proxy' drop-down list, select 'Yes'.

Figure 8-40: 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 288).

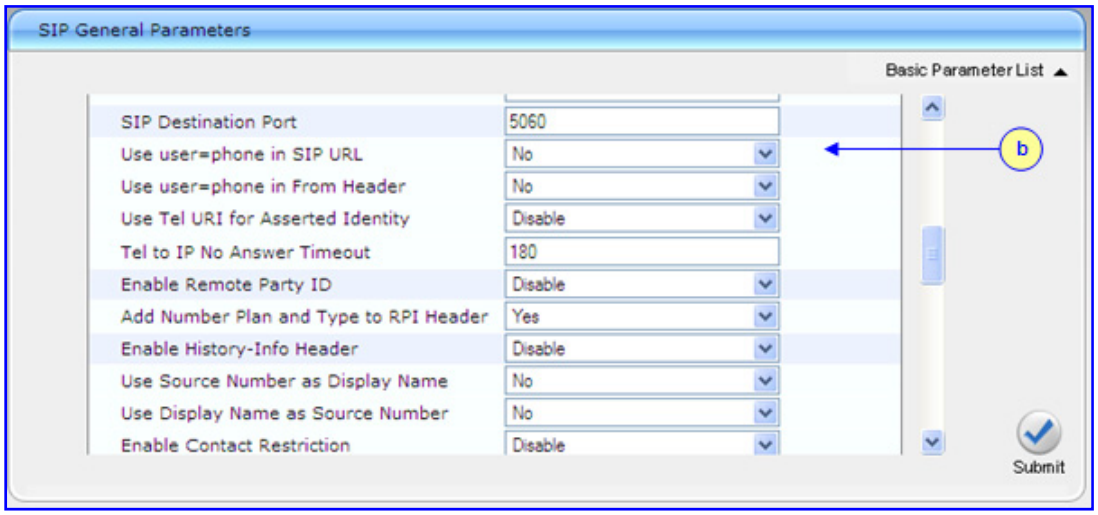
Figure 8-41: Defining Proxy Server for Gateway Application



   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 to not 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 8-42: Disabling user=phone in SIP URL



   c. Click **Submit**.

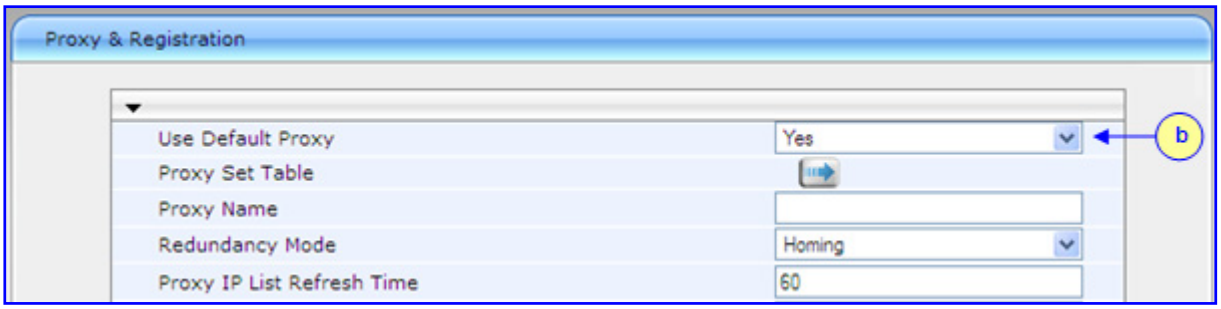
8.3.3.4.2 Gateway with SAS Redundant Mode

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 8-43: Enabling Proxy Server for Gateway Application

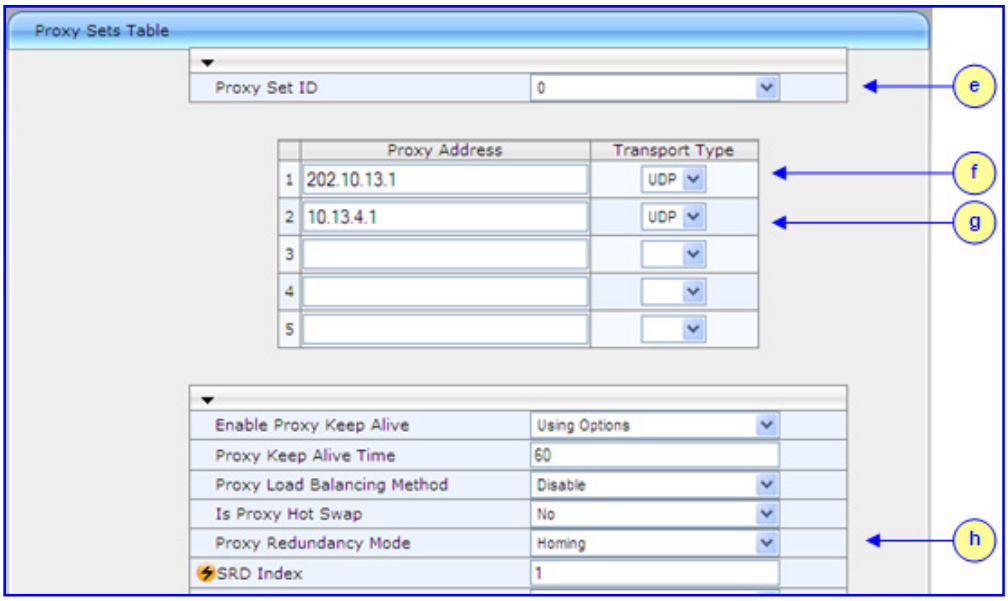


   c. Click **Submit**.
   d. Open the 'Proxy Sets Table' page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).
   e. From the 'Proxy Set ID' drop-down list, select '0'.
   f. In the first 'Proxy Address' field, enter the IP address of the external proxy server.

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 288).

h. From the 'Proxy Redundancy Mode' drop-down list, select 'Homing'.

Figure 8-44: Defining Proxy Servers for Gateway Application



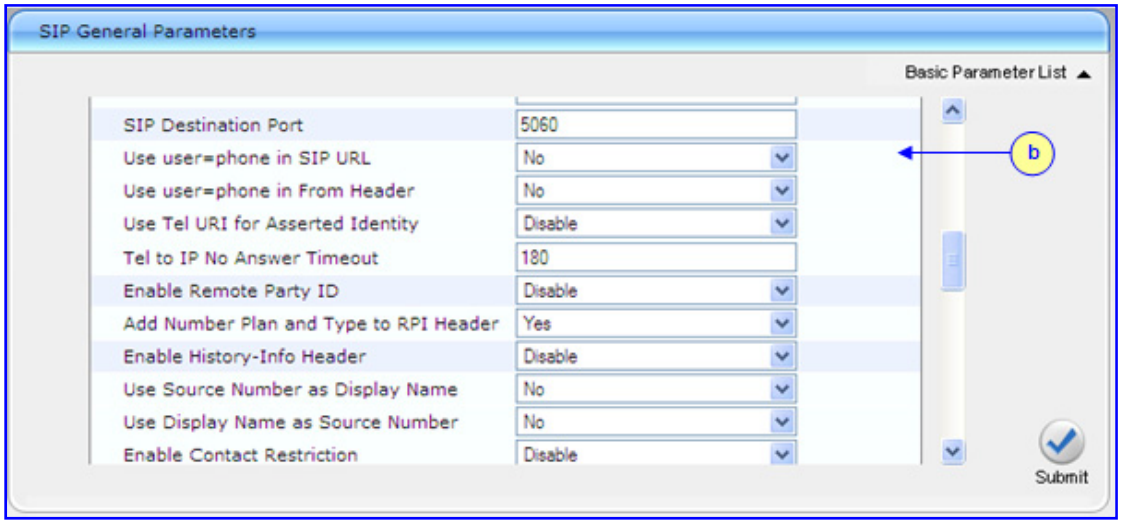
i. Click **Submit**.

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 to not 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*.)

Figure 8-45: Disabling user=phone in SIP URL



c. Click **Submit**.

8.3.3.5 Advanced SAS Configuration

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

- Manipulating incoming SAS Request-URI user part of REGISTER message (see "Manipulating URI user part of Incoming REGISTER" on page 295)
- Manipulating destination number of incoming SAS INVITE messages (see "Manipulating Destination Number of Incoming INVITE" on page 296)
- Defining SAS routing rules based on the SAS Routing table (see "SAS Routing Based on SAS Routing Table" on page 298)
- Blocking unregistered SAS UA's (see "Blocking Calls from Unregistered SAS Users" on page 298)
- Defining SAS emergency calls (see "Configuring SAS Emergency Calls" on page 299)
- Adding SIP Record-Route header to INVITE messages (see "Adding SIP Record-Route Header to SIP INVITE" on page 300)
- Replacing SIP Contact header (see "Replacing Contact Header for SIP Messages" on page 300)

8.3.3.5.1 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,SUBSCRIBE,
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)

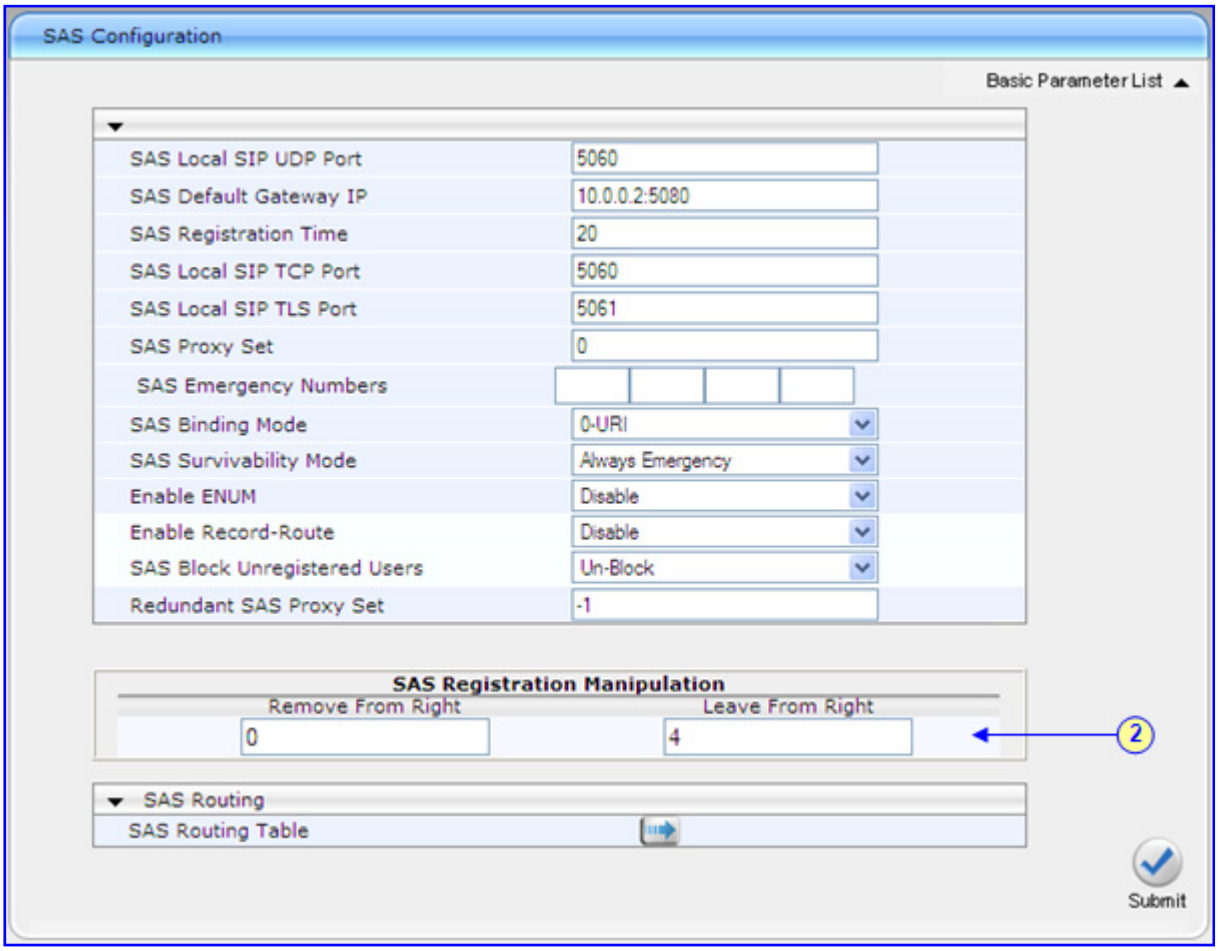
- **Contact:** 976653434@10.10.10.10

The procedure below describes how to configure the manipulation example scenario above (relevant *ini* parameter is SASRegistrationManipulation):

➢ **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. In the SAS Registration Manipulation table, in the 'Leave From Right' field, enter the number of digits (e.g., 4) to leave from the right side of the user part. (The 'Leave From Right' 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 8-46: Manipulating User Part in Incoming REGISTER



3. Click **Submit**.

8.3.3.5.2 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 whose 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 destination number in SAS emergency state:**

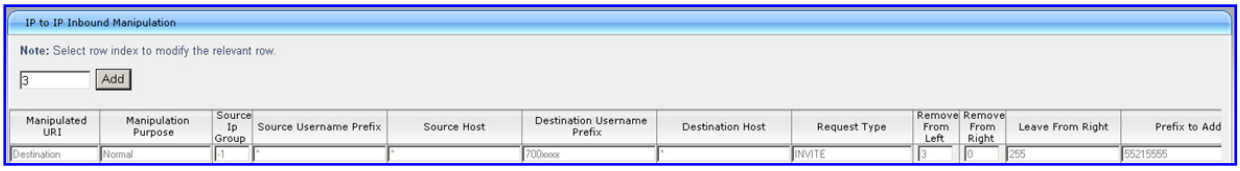
1. Load an *ini* file to the device with the following setting to enable inbound manipulation:

```
SASInboundManipulationMode = 1
```

2. Open the 'SAS Configuration' page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
3. Click the **IP to IP Inbound Manipulation Table** button to open the 'IP to IP Inbound Manipulation' page.
4. Enter a table index number, and then click **Add**.
5. Define the rules as required, and then click **Apply**.

The figure below displays a manipulation rule for the example scenario described above whereby the destination number "7001234" is changed to "552155551234":

Figure 8-47: Manipulating INVITE Destination Number



In the figure above, the following configuration is done:

- **Manipulated URI field:** 'Destination'
- **Destination Username Prefix field:** '700xxxx'
- **Request Type field:** 'INVITE'
- **Remove From Left field:** '3'
- **Prefix to Add field:** '55215555'

Notes:

- The 'Source IP Group' field must not be configured; leave it at '-1'.
- The 'Is Additional Manipulation' field must be set to '0'.
- The 'Manipulation Purpose' field must be set to 'Normal'.
- For a detailed description of the fields in the 'IP to IP Inbound Manipulation' table, see Configuring IP-to-IP Inbound Manipulations. This table is currently located under the **SBC** menu.

8.3.3.5.3 SAS Routing Based on SAS Routing Table

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

- SAS in normal state, if the SASSurvivabilityMode parameter is set to 4
- SAS in emergency state, if the SASSurvivabilityMode parameter is not set to 4

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

For a detailed description of the SAS Routing table, see "Configuring IP2IP Routing Table (SAS)" on page 163.

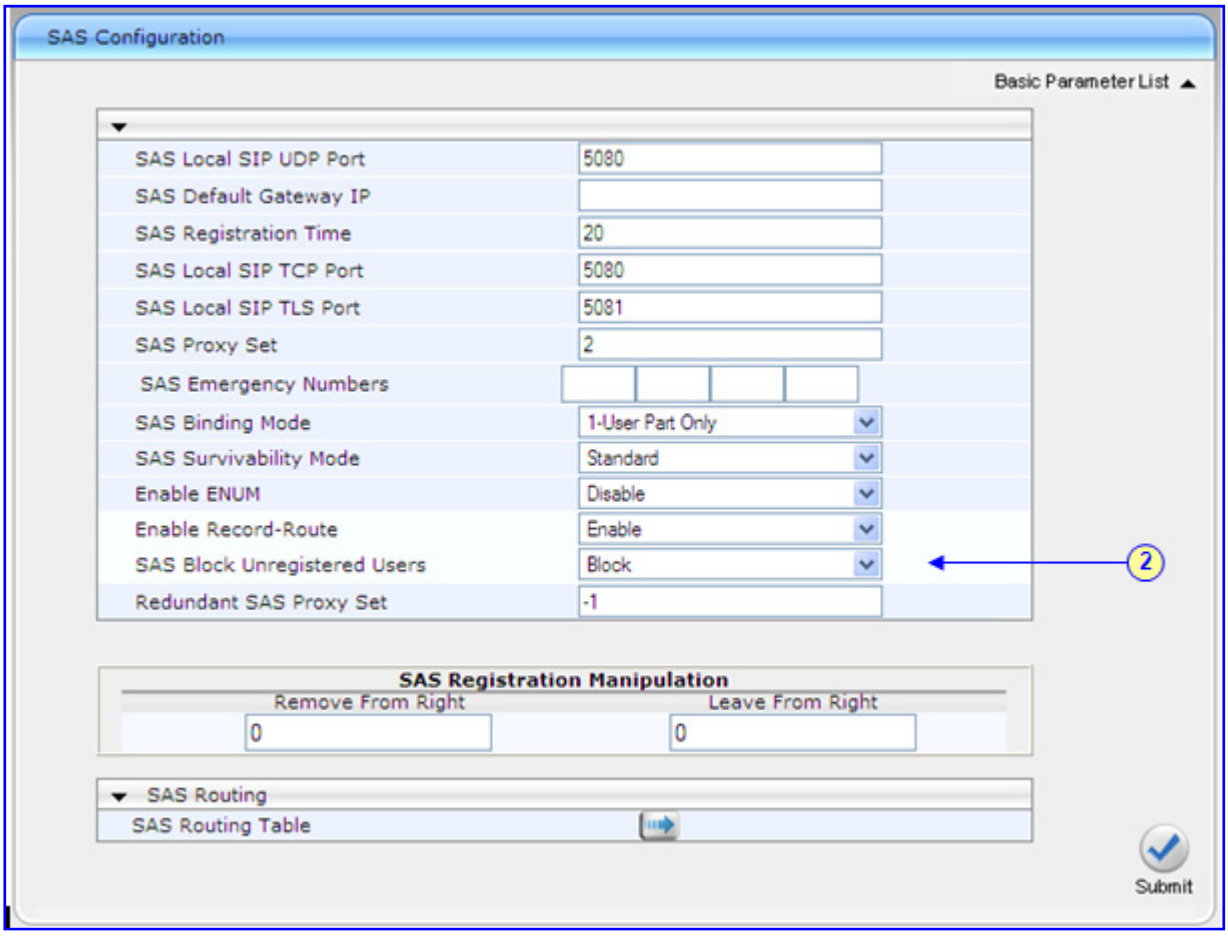
8.3.3.5.4 Blocking Calls from Unregistered SAS Users

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'.

Figure 8-48: Blocking Unregistered SAS Users



8.3.3.5.5 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). Therefore, 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 286). 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.

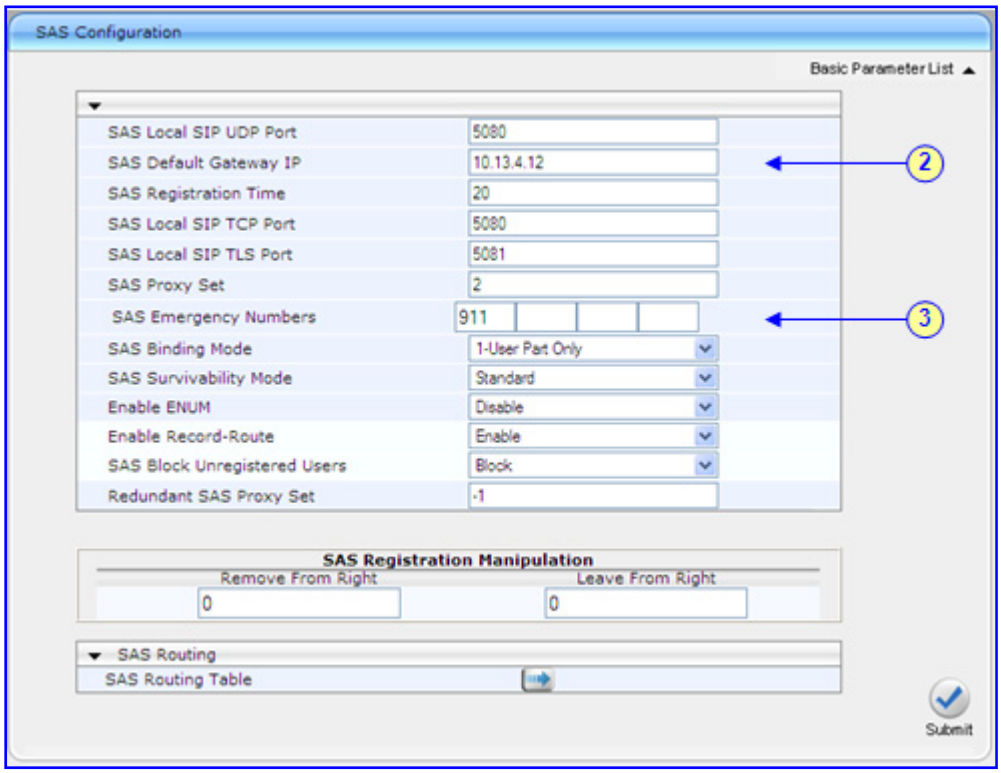
➢ **To configure SAS emergency numbers:**

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 8-49: Configuring SAS Emergency Numbers



4. Click **Submit**.

8.3.3.5.6 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 the 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).

This feature can only be configured using the SASEnableRecordRoute *ini* file parameter.

Note: This feature is applicable only to SAS outbound mode.

When this feature is enabled, the SIP Record-Route header includes the URI "lr" parameter. The presence of this parameter indicates loose routing; the lack of it indicates strict routing. For example:

- **Loose routing:**

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

- **Strict routing:**

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

8.3.3.5.7 Replacing Contact Header for SIP Messages

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

Note:

- This feature is applicable only to 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 only be configured using the SASEnableContactReplace *ini* file parameter.

- [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.

8.3.4 Viewing Registered SAS Users

You can view all the users that are registered in the SAS registration database. This is displayed in the 'SAS/SBC Registered Users' page, as described in "Viewing SAS/SBC Registered Users" on page 187. The maximum number of users that can be registered in the database is 25.

8.4 General

8.4.1 Event Notification using X-Detect Header

The device supports the sending of notifications to a remote party notifying the occurrence (or detection) of certain events on the media stream. Event detection and notifications is performed using the SIP X-Detect message header and only when establishing a SIP dialog.

For supporting some events, certain device configurations need to be performed. The table below lists the supported event types (and subtypes) and the corresponding device configurations, if required:

Table 8-4: Supported X-Detect Event Types

Events Type	Subtype	Required Configuration
CPT	SIT-NC SIT-IC SIT-VC SIT-RO Busy Reorder Ringtone beep	SITDetectorEnable = 1 UserDefinedToneDetectorEnable = 1 **Notes:** ▪ Ensure that the CPT file is configured with the required tone type. ▪ On beep detection, a SIP INFO message is sent with type AMD/CPT and subtype beep. ▪ The beep detection must be started using regular X-detect extension, with AMD or CPT request.
FAX	CED	(IsFaxUsed ≠ 0) or (IsFaxUsed = 0, and FaxTransportMode ≠ 0)
	modem	VxxModemTransportType = 3
PTT	voice-start voice-end	EnableDSPIPMDetectors = 1

The device can detect and report the following Special Information Tones (SIT) types from the PSTN:

- SIT-NC (No Circuit found)
- SIT-IC (Operator Intercept)
- SIT-VC (Vacant Circuit - non-registered number)
- SIT-RO (Reorder - System Busy)

There are additional three SIT tones that are detected as one of the above SIT tones:

- The NC* SIT tone is detected as NC
- The RO* SIT tone is detected as RO
- The IO* SIT tone is detected as VC

The device can map these SIT tones to a Q.850 cause and then map them to SIP 5xx/4xx responses, using the parameters SITQ850Cause, SITQ850CauseForNC, SITQ850CauseForIC, SITQ850CauseForVC, and SITQ850CauseForRO.

Table 8-5: Special Information Tones (SITs) Reported by the device

Special Information Tones (SITs) Name	Description	First Tone Frequency Duration		Second Tone Frequency Duration		Third Tone Frequency Duration	
		(Hz)	(ms)	(Hz)	(ms)	(Hz)	(ms)
NC1	No circuit found	985.2	380	1428.5	380	1776.7	380
IC	Operator intercept	913.8	274	1370.6	274	1776.7	380
VC	Vacant circuit (non registered number)	985.2	380	1370.6	274	1776.7	380
RO1	Reorder (system busy)	913.8	274	1428.5	380	1776.7	380
NC*	-	913.8	380	1370.6	380	1776.7	380
RO*	-	985.2	274	1370.6	380	1776.7	380
IO*	-	913.8	380	1428.5	274	1776.7	380

For example:

```
INFO sip:5001@10.33.2.36 SIP/2.0
Via: SIP/2.0/UDP 10.33.45.65;branch=z9hG4bKac2042168670
Max-Forwards: 70
From: <sip:5000@10.33.45.65;user=phone>;tag=1c1915542705
To: <sip:5001@10.33.2.36;user=phone>;tag=WQJNIDDPCOKAPIDSCOTG
Call-ID: AIFHPETLLMVVFWPDXUHD@10.33.2.36
CSeq: 1 INFO
Contact: <sip:2206@10.33.45.65>
Supported: em,timer,replaces,path,resource-priority
Content-Type: application/x-detect
Content-Length: 28
Type= CPT
SubType= SIT-IC
```

The X-Detect event notification process is as follows:

1. For IP-to-Tel or Tel-to-IP calls, the device receives a SIP request message (using the X-Detect header) that the remote party wishes to detect events on the media stream. For incoming (IP-to-Tel) calls, the request must be indicated in the initial INVITE and responded to either in the 183 response (for early dialogs) or in the 200 OK response (for confirmed dialogs). For outgoing calls (Tel-to-IP), the request may be received in the 183 (for early dialogs) and responded to in the PRACK, or received in the 200 OK (for confirmed dialogs) and responded to in the ACK.
2. Once the device receives such a request, it sends a SIP response message (using the X-Detect header) to the remote party, listing all supported events that can be detected. The absence of the X-Detect header indicates that no detections are available.
3. Each time the device detects a supported event, the event is notified to the remote party by sending an INFO message with the following message body:
   - Content-Type: application/X-DETECT
   - Type = [CPT | FAX | PTT…]
   - Subtype = xxx (according to the defined subtypes of each type)

Below is an example of SIP messages using the X-Detect header:

```
INVITE sip:101@10.33.2.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
Max-Forwards: 70
From: "anonymous" <sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:100@10.33.2.53>
X- Detect: Request=CPT,FAX
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
From: "anonymous" <sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>;tag=1c19282
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:101@10.33.2.53>
X- Detect: Response=CPT,FAX
INFO sip:101@10.33.2.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
Max-Forwards: 70
From: "anonymous" <sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:100@10.33.2.53>
X- Detect: Response=CPT,FAX
Content-Type: Application/X-Detect
Content-Length: xxx
Type = CPT
Subtype = SIT
```

8.4.2 Supported RADIUS Attributes

The following table provides explanations on the RADIUS attributes included in the communication packets transmitted between the device and a RADIUS Server.

Table 8-6: Supported RADIUS Attributes

Attribute Number	Attribute Name	VSA No.	Purpose	Value Format	Example	AAA[1]
Request Attributes						
1	User-Name		Account number or calling party number or blank	String up to 15 digits long	5421385747	Start Acc Stop Acc
4	NAS-IP-Address		IP address of the requesting device	Numeric	192.168.14.43	Start Acc Stop Acc
6	Service-Type		Type of service requested	Numeric	1: login	Start Acc Stop Acc
26	H323-Incoming-Conf-Id	1	SIP call identifier	Up to 32 octets		Start Acc Stop Acc
26	H323-Remote-Address	23	IP address of the remote gateway	Numeric		Stop Acc
26	H323-Conf-ID	24	H.323/SIP call identifier	Up to 32 octets		Start Acc Stop Acc
26	H323-Setup-Time	25	Setup time in NTP format 1	String		Start Acc Stop Acc
26	H323-Call-Origin	26	The call's originator: Answering (IP) or Originator (PSTN)	String	Answer, Originate etc	Start Acc Stop Acc
26	H323-Call-Type	27	Protocol type or family used on this leg of the call	String	VoIP	Start Acc Stop Acc
26	H323-Connect-Time	28	Connect time in NTP format	String		Stop Acc
26	H323-Disconnect-Time	29	Disconnect time in NTP format	String		Stop Acc
26	H323-Disconnect-Cause	30	Q.931 disconnect cause code	Numeric		Stop Acc
26	H323-Gw-ID	33	Name of the gateway	String	SIPIDString	Start Acc Stop Acc
26	SIP-Call-ID	34	SIP Call ID	String	abcde@ac.com	Start Acc Stop Acc

Attribute Number	Attribute Name	VSA No.	Purpose	Value Format	Example	AAA[1]
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			String	8004567145	Start Acc
			Destination phone number	String	2427456425	Stop Acc
			Calling Party Number (ANI)	String	5135672127	Start Acc Stop Acc
			Account Request Type (start or stop) **Note:** 'start' isn't supported on the Calling Card application.	Numeric	1: start, 2: stop	Start Acc Stop Acc
			No. of seconds tried in sending a particular record	Numeric	5	Start Acc Stop Acc
			Number of octets received for that call duration	Numeric		Stop Acc
			Number of octets sent for that call duration	Numeric		Stop Acc
			A unique accounting identifier - match start & stop	String	34832	Start Acc Stop Acc
			For how many seconds the user received the service	Numeric		Stop Acc
			Number of packets received during the call	Numeric		Stop Acc
			Number of packets sent during the call	Numeric		Stop Acc
			Physical port type of device on which the call is active	String	0: Asynchronous	Start Acc Stop Acc
Response Attributes						
26	H323-Return-Code	103	The reason for failing authentication (0 = ok, other number failed)	Numeric	0 Request accepted	Stop Acc
44	Acct-Session-ID		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
```

8.4.3 Call Detail Record

The Call Detail Record (CDR) contains vital statistic information on calls made from the device. CDRs are generated at the end and optionally, at the beginning of each call (defined by the CDRReportLevel parameter). Once generated, they are sent to a Syslog server. The destination IP address for CDR logs is defined by the CDRSyslogServerIP parameter. For CDR in RADIUS format, see "Supported RADIUS Attributes" on page 304.

8.4.3.1 CDR Fields

The following table lists the supported CDR fields.

Table 8-7: Supported CDR Fields

Field Name	Description
ReportType	Report for either Call Started, Call Connected, or Call Released
Cid	Port Number
CallId	SIP Call Identifier
Trunk	Physical Trunk Number (always set to '-1', as not applicable)
BChan	Selected B-Channel (always set to '0', as not applicable)
ConId	SIP Conference ID
TG	Trunk Group Number
EPTyp	Endpoint Type
Orig	Call Originator (IP, Tel)
SourceIp	Source IP Address

Field Name	Description
DestIp	Destination IP Address
TON	Source Phone Number Type
NPI	Source Phone Number Plan
SrcPhoneNum	Source Phone Number
SrcNumBeforeMap	Source Number Before Manipulation
TON	Destination Phone Number Type
NPI	Destination Phone Number Plan
DstPhoneNum	Destination Phone Number
DstNumBeforeMap	Destination Number Before Manipulation
Durat	Call Duration
Coder	Selected Coder
Intrv	Packet Interval
RtpIp	RTP IP Address
Port	Remote RTP Port
TrmSd	Initiator of Call Release (IP, Tel, Unknown)
TrmReason	Termination Reason (see "Release Reasons in CDR" on page 308)
Fax	Fax Transaction during the Call
InPackets	Number of Incoming Packets
OutPackets	Number of Outgoing Packets
PackLoss	Local Packet Loss
RemotePackLoss	Number of Outgoing Lost Packets
UniqueId	unique RTP ID
SetupTime	Call Setup Time
ConnectTime	Call Connect Time
ReleaseTime	Call Release Time
RTPdelay	RTP Delay
RTPjitter	RTP Jitter
RTPssrc	Local RTP SSRC
RemoteRTPssrc	Remote RTP SSRC
RedirectReason	Redirect Reason
TON	Redirection Phone Number Type
MeteringPulses	Number of Generated Metering Pulses
NPI	Redirection Phone Number Plan
RedirectPhonNum	Redirection Phone Number

8.4.3.2 Release Reasons in CDR

The possible reasons for call termination 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_CONFERENCE_RESOURCES_LEFT"
- "RELEASE_BECAUSE_CONFERENCE_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_UKNOWN_ERROR"
- "RELEASE_BECAUSE_HELD_TIMEOUT"

8.4.4 RTP Multiplexing (ThroughPacket)

The device supports a proprietary method to aggregate RTP streams from several channels. This reduces the bandwidth overhead caused by the attached Ethernet, IP, UDP, and RTP headers and reduces the packet/data transmission rate. This option reduces the load on network routers and can typically save 50% (e.g., for G.723) on IP bandwidth. RTP Multiplexing (ThroughPacket™) is accomplished by aggregating payloads from several channels that are sent to the same destination IP address into a single IP packet.

RTP multiplexing can be applied to the entire device (see "Configuring RTP/RTCP Settings" on page 100) or to specific IP destinations using the IP Profile feature (see "Configuring IP Profiles" on page 122).

To enable RTP Multiplexing, set the parameter RemoteBaseUDPPort to a non-zero value. Note that the value of RemoteBaseUDPPort on the local device must equal the value of BaseUDPPort of the remote device. The device uses these parameters to identify and distribute the payloads from the received multiplexed IP packet to the relevant channels.

When RTP Multiplexing is used, call statistics are unavailable (since there is no RTCP flow).

Notes:

- RTP Multiplexing must be enabled on both devices.
- When VLANs are implemented, the RTP Multiplexing mechanism is not supported.

9 VoIP Networking Capabilities

This section provides an overview of the device's VoIP networking capabilities.

9.1 Ethernet Interface Configuration

The device's Ethernet connection can be configured (using the *ini* file parameter EthernetPhyConfiguration) for one of the following modes:

- **Manual mode:**
  - 10Base-T Full-Duplex
  - 100Base-TX Half-Duplex or 100Base-TX Full-Duplex
- **Auto-Negotiation:** chooses common transmission parameters such as speed and duplex mode

The Ethernet connection should be configured according to the following recommended guidelines:

- When the device's Ethernet port is configured for Auto-Negotiation, the opposite port must also operate in Auto-Negotiation. Auto-Negotiation falls back to Half-Duplex mode when the opposite port is not in Auto-Negotiation mode, but the speed in this mode is always configured correctly. Configuring the device to Auto-Negotiation mode while the opposite port is set manually to Full-Duplex is invalid as it causes the device to fall back to Half-Duplex mode while the opposite port is Full-Duplex. Any mismatch configuration can yield unexpected functioning of the Ethernet connection.
- When configuring the device's Ethernet port manually, the same mode (i.e., Half Duplex or Full Duplex) and speed must be configured on the remote Ethernet port. In addition, when the device's Ethernet port is configured manually, it is invalid to set the remote port to Auto-Negotiation**.** Any mismatch configuration can yield unexpected functioning of the Ethernet connection.
- It's recommended to configure the port for best performance and highest bandwidth (i.e., Full Duplex with 100Base-TX), but at the same time adhering to the guidelines listed above.

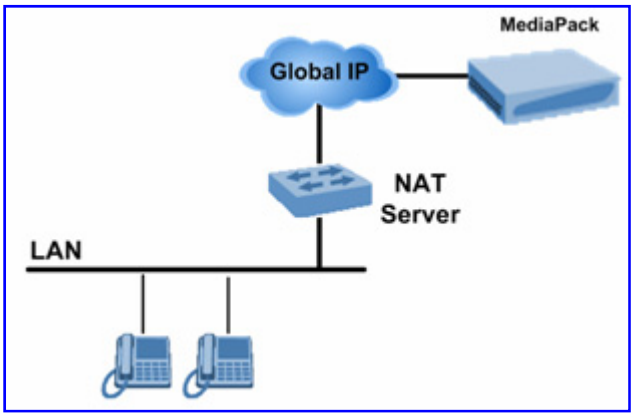
Note that when remote configuration is performed, the device should be in the correct Ethernet setting prior to the time this parameter takes effect. When, for example, the device is configured using BootP/TFTP, the device performs many Ethernet-based transactions prior to reading the *ini* file containing this device configuration parameter. To resolve this problem, the device always uses the last Ethernet setup mode configured. In this way, if you want to configure the device to operate in a new network environment in which the current Ethernet setting of the device is invalid, you should first modify this parameter in the current network so that the new setting holds next time the device is restarted. After reconfiguration has completed, connect the device to the new network and restart it. As a result, the remote configuration process that occurs in the new network uses a valid Ethernet configuration.

9.2 NAT (Network Address Translation) Support

Network Address Translation (NAT) is a mechanism that maps a set of internal IP addresses used within a private network to global IP addresses, 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); (2) Better network security by hiding its internal architecture.

The following figure illustrates the device's supported NAT architecture.

Figure 9-1: Nat Functioning



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 and the NAT server can't modify SIP messages and therefore, can't change local to global addresses. Two different streams traverse through NAT: signaling and media. A device (located behind a NAT) that initiates a signaling path has problems in receiving incoming signaling responses (they are blocked by the NAT server). Furthermore, the initiating device must notify the receiving device where to send the media.

To resolve these issues, the following mechanisms are available:

- STUN (see STUN on page 312)
- First Incoming Packet Mechanism (see "First Incoming Packet Mechanism" on page 313)
- RTP No-Op packets according to the avt-rtp-noop draft (see "No-Op Packets" on page 313)

For information on SNMP NAT traversal, refer to the *Product Reference Manual*.

9.2.1 STUN

Simple Traversal of UDP through NATs (STUN), based on RFC 3489 is a client / server protocol that solves most of the NAT traversal problems. The STUN server operates in the public Internet and the STUN clients are embedded in end-devices (located behind NAT). STUN is used both for the signaling and the media streams. STUN works with many existing NAT types and does not require any special behavior.

STUN enables the device to discover the presence (and types) of NATs and firewalls located between it and the public Internet. It provides the device with the capability to determine the public IP address and port allocated to it by the NAT. This information is later embedded in outgoing SIP / SDP messages and enables remote SIP user agents to reach the device. It also discovers the binding lifetime of the NAT (the refresh rate necessary to keep NAT 'Pinholes' open).

On startup, the device sends a STUN Binding Request. The information received in the STUN Binding Response (IP address:port) is used for SIP signaling. This information is updated every user-defined period (NATBindingDefaultTimeout).

At the beginning of each call and if STUN is required (i.e., not an internal NAT call), the media ports of the call are mapped. The call is delayed until the STUN Binding Response (that includes a global IP:port) for each media (RTP, RTCP and T.38) is received.

To enable STUN, perform the following:

- Enable the STUN feature (by setting the *ini* file parameter EnableSTUN to 1).
- Define the STUN server address using one of the following methods:
  - Define the IP address of the primary and the secondary (optional) STUN servers (using the *ini* file parameters STUNServerPrimaryIP and STUNServerSecondaryIP). If the primary STUN server isn't available, the device attempts to communicate with the secondary server.
  - Define the domain name of the STUN server using the *ini* file parameter StunServerDomainName. The STUN client retrieves all STUN servers with an SRV query to resolve this domain name to an IP address and port, sort the server list, and use the servers according to the sorted list.
- Use the *ini* file parameter NATBindingDefaultTimeout to define the default NAT binding lifetime in seconds. STUN is used to refresh the binding information after this time expires.

Notes:

- STUN only applies to UDP (it doesn't support TCP and TLS).
- STUN can't be used when the device is located behind a symmetric NAT.
- Use either the STUN server IP address (STUNServerPrimaryIP) or domain name (STUNServerDomainName) method, with priority to the first one.

9.2.2 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 incoming RTP/RTCP/T.38 stream with the IP address and UDP port of the remote device. If the two are not identical, the transmitter modifies the sending address to correspond with the address of the incoming stream. The RTP, RTCP and T.38 can thus have independent destination IP addresses and UDP ports.

You can disable the NAT mechanism by setting the *ini* file parameter DisableNAT to 1. The two parameters EnableIpAddrTranslation and EnableUdpPortTranslation allow you to specify the type of compare operation that occurs on the first incoming packet. To compare only the IP address, set EnableIpAddrTranslation to 1, and EnableUdpPortTranslation to 0. In this case, if the first incoming packet arrives with only a difference in the UDP port, the sending addresses won't change. If both the IP address and UDP port need to be compared, then both parameters need to be set to 1.

9.2.3 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 performed using the *ini* file parameter NoOpInterval. For a description of the RTP No-Op *ini* file parameters, see "Networking Parameters" on page 333.

- **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 333). AudioCodes' 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.

9.3 IP Multicasting

The device supports IP Multicasting level 1 according to RFC 2236 (i.e., IGMP version 2) for RTP channels. The device is capable of transmitting and receiving Multicast packets.

9.4 Robust Receipt of Media Streams

This mechanism filters out unwanted RTP streams that are sent to the same port number on the device. These multiple RTP streams can result from traces of previous calls, call control errors, and deliberate attacks. When more than one RTP stream reaches the device on the same port number, the device accepts only one of the RTP streams and rejects the rest of the streams.

The RTP stream is selected according to the following: The first packet arriving on a newly opened channel sets the source IP address and UDP port from which further packets are received. Thus, the source IP address and UDP port identify the currently accepted stream. If a new packet arrives whose source IP address or UDP port are different to the currently accepted RTP stream, one of the following occurs:

- The device reverts to the new RTP stream when the new packet has a source IP address and UDP port that are the same as the remote IP address and UDP port that were stated during the opening of the channel.
- The packet is dropped when the new packet has any other source IP address and UDP port.

9.5 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.

9.6 Simple Network Time Protocol Support

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) and the update interval are user-defined (using the *ini* file parameters NTPServerIP and NTPUpdateInterval respectively), or an SNMP MIB object (refer to the *Product Reference Manual*).

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 using the *ini* file parameter NTPServerUTCOffset, or via an SNMP MIB object (refer to the *Product Reference Manual*).

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.

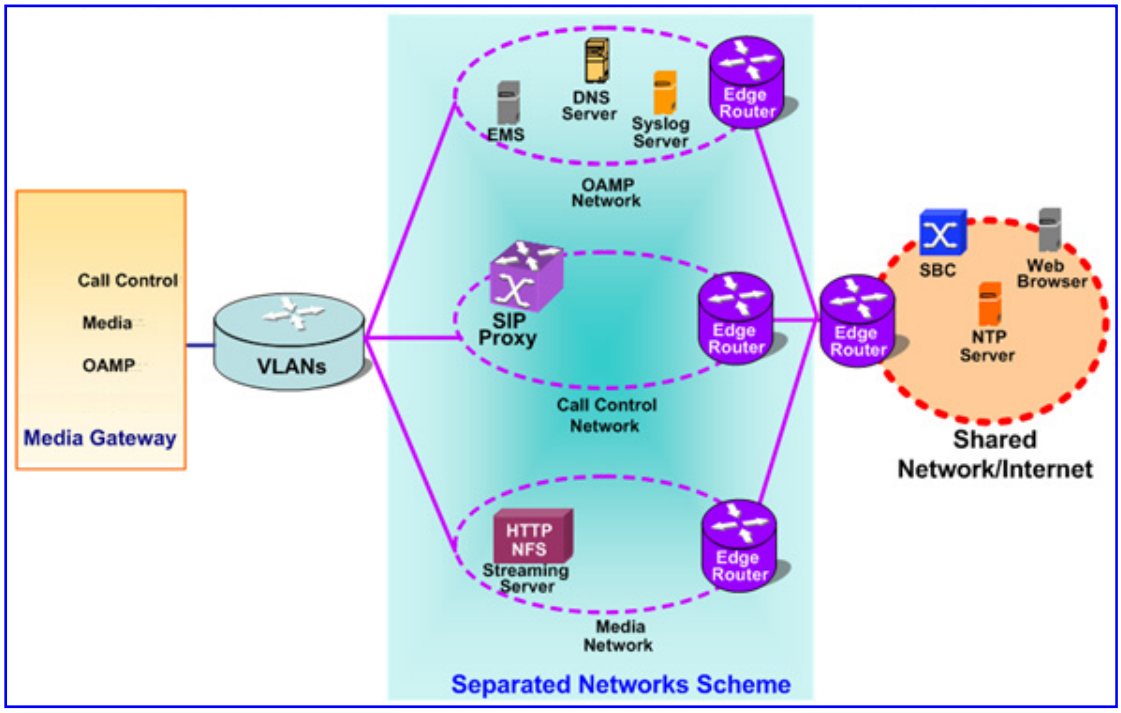
9.7 Network Configuration

The device allows you to configure up to 16 different IP addresses with associated VLANs, using the Multiple Interface table. Complementing this table is the Routing table, which allows you to define static routing rules for non-local hosts/subnets. This section describes the various network configuration options offered by the device.

9.7.1 Multiple Network Interfaces and VLANs

A need often arises to have logically separated network segments for various applications (for administrative and security reasons). This can be achieved by employing Layer-2 VLANs and Layer-3 subnets.

Figure 9-2: Multiple Network Interfaces



The figure depicts a typical configuration featuring in which the device is configured with three network interfaces for:

- Operations, Administration, Maintenance, and Provisioning (OAMP) applications
- Call Control applications
- Media

It is connected to a VLAN-aware switch, which is used for directing traffic from (and to) the device to three separated Layer-3 broadcast domains according to VLAN tags (middle pane).

The Multiple Interfaces scheme allows the configuration of up to 16 different IP addresses, each associated with a unique VLAN ID. The configuration is performed using the Multiple Interface table, which is configurable using the *ini* file, Web, and SNMP interfaces.

9.7.1.1 Overview of Multiple Interface Table

The Multiple Interfaces scheme allows you to define up to 16 different IP addresses and VLANs in a table format, as shown below:

Table 9-1: Multiple Interface Table

Index Mode	Application	Interface	IP Address	Prefix Length	Default Gateway	VLAN ID	Interface Name
0	OAMP	IPv4	10.31.174.50	16	0.0.0.0	4	ManagementIF
1	Control	IPv4	10.32.174.50	16	0.0.0.0	5	ControlIF
2	Media	IPv4	10.33.174.50	16	10.33.0.1	6	Media1IF
3	Media	IPv4	10.34.174.50	16	0.0.0.0	7	Media2IF
4	Media	IPv4	10.35.174.50	16	10.35.0.1	8	Media3IF
5	Media	IPv4	10.36.174.50	16	0.0.0.0	9	Media4IF
6	Media	IPv4	10.37.174.50	16	0.0.0.0	10	Media5IF
7	Media	IPv4	10.38.174.50	16	0.0.0.0	11	Media6IF
8	Media	IPv4	10.39.174.50	16	10.39.0.1	12	Media7IF
9	Media	IPv4	10.40.174.50	16	10.40.0.1	13	Media8IF
10	Media & Control	IPv4	10.41.174.50	16	0.0.0.0	14	MediaCtrl9IF
11	Media	IPv4	10.42.174.50	16	0.0.0.0	15	Media10IF
12	Media	IPv4	10.43.174.50	16	10.43.0.1	16	Media11IF
13	Media	IPv4	10.44.174.50	16	0.0.0.0	17	Media12IF
14	Media	IPv4	10.45.174.50	16	10.45.0.1	18	Media13IF
15	Media & Control	IPv4	10.46.174.50	16	0.0.0.0	19	MediaCtrl14IF

Complementing the network configuration are some VLAN-related parameters, determining if VLANs are enabled and the 'Native' VLAN ID (see the sub-sections below) as well as VLAN priorities and DiffServ values for the supported Classes Of Service (see Quality of Service Parameters on page 320).

9.7.1.2 Columns of the Multiple Interface Table

Each row of the table defines a logical IP interface with its own IP address, subnet mask (represented by Prefix Length), VLAN ID (if VLANs are enabled), name, and application types that are allowed on this interface. Multiple interfaces can be defined with a default gateway. Traffic from this interface destined to a subnet which does not meet any of the routing rules (either local or static routes) are forwarded to this gateway (as long this application type is allowed on this interface). See "Gateway Column" on page 319 for more details.

9.7.1.2.1 Index Column

This column holds the index of each interface. Possible values are 0 to 15. Each interface index must be unique.

9.7.1.2.2 Application Types Column

This column defines the types of applications that are allowed on this interface:

- OAMP – Operations, Administration, Maintenance and Provisioning applications such as Web, Telnet, SSH, SNMP
- CONTROL – Call Control protocols (i.e., SIP)
- MEDIA – RTP streams of voice
- Various combinations of the above mentioned types

The following table shows the possible values of this column and their descriptions:

Table 9-2: Application Types

Value	Description
0	OAMP: only OAMP applications are allowed on this interface.
1	MEDIA: only Media (RTP) are allowed on this interface.
2	CONTROL: only Call Control applications are allowed on this interface.
3	OAMP & MEDIA: only OAMP and Media (RTP) applications are allowed on this interface.
4	OAMP & CONTROL: only OAMP and Call Control applications are allowed on this interface.
5	MEDIA & CONTROL: only Media (RTP) and Call Control applications are allowed on this interface.
6	OAMP, MEDIA & CONTROL: all of the application types are allowed on this interface.

For valid configuration guidelines, see "Multiple Interface Table Configuration Summary and Guidelines" on page 323 for more information.

9.7.1.2.3 Interface Mode Column

The Interface Mode column determines the method that this interface uses to acquire its IP address. For IPv4 Manual IP Address assignment, use "IPv4 Manual" (10).

9.7.1.2.4 IP Address and Prefix Length Columns

These columns allow the user to configure an IPv4 IP address and its related subnet mask.

The Prefix Length column holds the 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, in other words, 192.168.0.0/16 is synonymous with 192.168.0.0 and a subnet 255.255.0.0 (Refer to http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing for more information).

This CIDR notation lists the number of '1' bits in the subnet mask. So, a subnet mask of 255.0.0.0 (when broken down to its binary format) is represented by a prefix length of 8 (11111111 00000000 00000000 00000000), and a subnet mask of 255.255.255.252 is represented by a prefix length of 30 (11111111 11111111 11111111 11111100).

Each interface must have its own address space. Two interfaces may not share the same address space, or even part of it. The IP address should be configured as a dotted-decimal notation.

For IPv4 interfaces, the prefix length values range from 0 to 30.

OAMP Interface Address when Booting using BootP/DHCP: When booting using BootP/DHCP protocols, an IP address is obtained from the server. This address is used as the OAMP address for this session, overriding the address configured using the Multiple Interface table. The address specified for OAMP applications in the table becomes available when booting from flash again. This allows the device to operate with a temporary address for initial management and configuration while retaining the address to be used for deployment.

9.7.1.2.5 Gateway Column

This column defines a default gateway for each interface. A default gateway can be defined for each interface. When traffic is sent from this interface to an unknown destination (i.e., not in the same subnet and not defined for any static routing rule), it is forwarded to this default gateway. The default gateway's address must be on the same subnet as the interface address. A separate routing table allows configuring additional static routing rules. See "Routing Table" on page 325 for more details.

Note: In the example below, the default gateway (200.200.85.1) is available for the applications allowed on that Interface #1. Outgoing management traffic (originating on Interface #0) is never directed to this default gateway.

Table 9-3: Configured Default Gateway Example

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP	IPv4 Manual	192.168.85.14	16	0.0.0.0	100	Mgmt
1	Media & Control	IPv4 Manual	200.200.85.14	24	200.200.85.1	200	CntrlMedia

A separate routing table allows configuring static routing rules. Configuring the following routing rule enables OAMP applications to access peers on subnet 17.17.0.0 through the gateway 192.168.0.1.

Table 9-4: Separate Routing Table Example

Destination	Prefix Length	Gateway	Interface	Metric	Status
17.17.0.0	16	192.168.0.1	0	1	Active

9.7.1.2.6 VLAN ID Column

This column defines the VLAN ID for each interface. This column must hold a unique value for each interface of the same address family.

9.7.1.2.7 Interface Name Column

This column allows the configuration of a short string (up to 16 characters) to name this interface. This name is displayed in management interfaces (Web, CLI, and SNMP) and is used in the Media Realm table. This column must have a unique value for each interface (no two interfaces can have the same name) and must not be left blank.

9.7.1.3 Other Related Parameters

The Multiple Interface table allows you to configure interfaces and their related parameters such as VLAN ID, or interface name. This section lists additional parameters complementing this table functionality.

9.7.1.3.1 Booting using DHCP

The *DHCPEnable* parameter enables the device to boot while acquiring an IP address from a DHCP server. Note that when using this method, Multiple Interface table/VLANs and other advanced configuration options are disabled.

9.7.1.3.2 Enabling VLANs

The Multiple Interface table's column "VLAN ID" assigns a VLAN ID to each of the interfaces. Incoming traffic tagged with this VLAN ID are channeled to the related interface, and outgoing traffic from that interface are tagged with this VLAN ID. When VLANs are required, the parameter should be set to 1. The default value for this parameter is 0 (disabled).

9.7.1.3.3 'Native' VLAN ID

A 'Native' VLAN ID is the VLAN ID to which untagged incoming traffic are assigned. Outgoing packets sent to this VLAN are sent only with a priority tag (VLAN ID = 0). When the 'Native' VLAN ID is equal to one of the VLAN IDs configured in the Multiple Interface table (and VLANs are enabled), untagged incoming traffic are considered as an incoming traffic for that interface. Outgoing traffic sent from this interface are sent with the priority tag (tagged with VLAN ID = 0). When the 'Native' VLAN ID is different from any value in the "VLAN ID" column in the Multiple Interface table, untagged incoming traffic are discarded and all the outgoing traffic are fully tagged.

The 'Native' VLAN ID is configurable using the VlanNativeVlanId parameter (refer to the Setting up your System sub-section below). The default value of the 'Native' VLAN ID is 1.

Note: If *VlanNativeVlanId* is not configured (i.e., its default value of 1 occurs), but one of the interfaces has a VLAN ID configured to 1, this interface is still related to the 'Native' VLAN. If you do not wish to have a 'Native' VLAN ID, and want to use VLAN ID 1, ensure that the value of the *VlanNativeVlanId* parameter is different than any VLAN ID in the table.

9.7.1.3.4 Quality of Service Parameters

The device allows you to specify values for Layer-2 and Layer-3 priorities, by assigning values to the following service classes:

- Network Service class – network control traffic (ICMP, ARP)
- Premium Media service class – used for RTP Media traffic
- Premium Control Service class – used for Call Control traffic
- Gold Service class – used for streaming applications
- Bronze Service class – used for OAMP applications

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

Table 9-5: Quality of Service Parameters

Parameter	Description
Layer-2 Class Of Service Parameter (VLAN Tag Priority Field)	
VlanNetworkServiceClassPriority	Sets the priority for the Network service class content
VLANPremiumServiceClassMediaPriority	Sets the priority for the Premium service class content (media traffic)
VLANPremiumServiceClassControlPriority	Sets the priority for the Premium service class content (control traffic)
VLANGoldServiceClassPriority	Sets the priority for the Gold service class content (streaming traffic)
VLANBronzeServiceClassPriority	Sets the priority for the Bronze service class content (OAMP traffic)
Layer-3 Class Of Service Parameters (TOS/DiffServ)	
NetworkServiceClassDiffServ	Sets the DiffServ for the Network service class content
PremiumServiceClassMediaDiffServ	Defines the DiffServ value for Premium Media CoS content (media traffic).
PremiumServiceClassControlDiffServ	Defines the DiffServ value for Premium Control CoS content (Call Control applications).
GoldServiceClassDiffServ	Sets the DiffServ for the Gold service class content (streaming applications).
BronzeServiceClassDiffServ	Sets the DiffServ for the Bronze service class content (OAMP applications).

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

Table 9-6: 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
IPSec IKE	Determined by the service	Determined by the service
RTP traffic	Media	Premium media
RTCP traffic	Media	Premium media
T.38 traffic	Media	Premium media
SIP	Control	Premium control
SIP over TLS (SIPS)	Control	Premium control
Syslog	Management	Bronze
ICMP	Management	Determined by the initiator of the request
ARP listener	Determined by the initiator of the request	Network
SNMP Traps	Management	Bronze
DNS client	Varies according to DNS settings (EnableDNSasOAM): ▪ OAMP ▪ Control	Depends on traffic type: ▪ Control: Premium Control ▪ Management: Bronze
NTP	Varies according to NTP settings (EnableNTPasOAM): ▪ OAMP ▪ Control	Depends on traffic type: ▪ Control: Premium control ▪ Management: Bronze
NFS	NFSServers_VlanType in the NFSServers table	Gold

9.7.1.3.5 Applications with Assignable Application Type

Some applications can be associated with different application types in different setups. These application types are configurable. The applications listed below can be configured to one of two application types:

- DNS
- NTP

Table 9-7: Application Type Parameters

Parameter	Description
EnableDNSasOAM	Determines the application type for DNS services. ▪ **[1]** = OAMP (default) ▪ **[0]** = Control. **Note:** For this parameter to take effect, a device reset is required.
EnableNTPasOAM	Determines the application type for NTP services. ▪ **[1]** = OAMP (default) ▪ **[0]** = Control. **Note:** For this parameter to take effect, a device reset is required.

9.7.1.4 Multiple Interface Table Configuration Summary and Guidelines

Multiple Interface table configuration must adhere to the following rules:

- Up to 16 different interfaces may be defined.
- The indices used must be in the range between 0 and 15.
- Each interface must have its own subnet. Defining two interfaces with addresses in the same subnet (i.e. two interfaces with 192.168.0.1/16 and 192.168.100.1/16) is illegal.
- Subnets in different interfaces must not be overlapping in any way (i.e. defining two interfaces with 10.0.0.1/8 and 10.50.10.1/24 is invalid). Each interface must have its own address space.
- The Prefix Length replaces the dotted decimal Subnet Mask presentation. This column must have a value of 0-30 for IPv4 interfaces.
- Only one IPv4 interface with OAMP "Application Types" **must** be configured. At least one IPv4 interface with CONTROL "Application Types" **must** be configured. At least one IPv4 interface with MEDIA "Application Types" **must** be configured. These application types **may** be mixed (i.e. OAMP and CONTROL). Here are some examples for interface configuration:
  - One IPv4 interface with "Application Types" OAMP, MEDIA & CONTROL (without VLANs).
  - One IPv4 interface with "Application Types" OAMP, one other or more IPv4 interfaces with "Application Types" CONTROL, and one or more IPv4 interfaces with "Application Types" MEDIA (with VLANs).
  - One IPv4 interface with "Application Types" OAMP & MEDIA, one other or more IPv4 interfaces with "Application Types" MEDIA & CONTROL.
  - Other configurations are also possible while keeping to the above-mentioned rule.
- Each network interface may be defined with a default gateway. This default gateway address must be in the same subnet as the associated interface. Additional routing rules may be specified in the Routing table ("Routing Table" on page 325).
- The Interface Name column may have up to 16 characters. This column allows the user to name each interface with an easier name to associate the interface with. This column must have a unique value to each interface and must not be left blank.
- For IPv4 interfaces, the "Interface Mode" column must be set to "IPv4 Manual" (numeric value 10).
- When defining more than one interface of the same address family, VLANs must be enabled (the VlanMode should be set to 1).

- VLANs become available only when booting the device from flash. When booting using BootP/DHCP protocols, VLANs are disabled to allow easier maintenance access. In this scenario, multiple network interface capabilities are unavailable.
- The 'Native' VLAN ID may be defined using the 'VlanNativeVlanId' parameter. This relates untagged incoming traffic as if reached with a specified VLAN ID. Outgoing traffic from the interface which VLAN ID equals to the 'Native' VLAN ID are tagged with VLAN ID 0 (priority tag).
- Quality of Service parameters specify the priority field for the VLAN tag (IEEE 802.1p) and the DiffServ field for the IP headers. These specifications relate to service classes.
- When booting using BootP/DHCP protocols, the address received from the BootP/DHCP server acts as a temporary OAMP address, regardless of the address specified in the Multiple Interface table. This configured address becomes available when booting from flash.
- Network Configuration changes are offline. The new configuration should be saved and becomes available at the next startup.

Upon system 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. Please be sure to follow the Syslog messages that the device sends in system startup to see if any errors occurred.

Note: When configuring the device using the Web interface, it is possible to perform a quick validation of the configured Multiple Interface table and VLAN definitions, by clicking the **Done** button in the Multiple Interface Table Web page. It is highly recommended to perform this when configuring Multiple Interfaces and VLANs, using the Web Interface to ensure the configuration is complete and valid.

9.7.1.5 Troubleshooting the Multiple Interface Table

If any of the Multiple Interface table guidelines are violated, the device falls back to a "safe mode" configuration, consisting of a single IPv4 interface without VLANs. 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, and MEDIA) is missing in the IPv4 interfaces.
- There are too many interfaces with "Application Types" of OAMP. Only one interface defined but the "Application Types" column is not set to "OAM + Media + Control" (numeric value 6).
- An IPv4 interface was defined with "Interface Type" different than "IPv4 Manual" (10).
- Two interfaces have the exact VLAN ID value, while VLANs are enabled.
- Two interfaces have the same name.
- Two interfaces share the same address space or subnet.

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

- Trying to access the device with VLAN tags while booting from BootP/DHCP.
- Trying to access the device with untagged traffic when VLANs are on and Native VLAN is not configured properly.
- Routing Table is not configured properly.

9.7.2 Static Routing Table

The IP Routing table allows you to configure static routing rules. You may define up to 30 different routing rules, using the *ini* file, Web interface, and SNMP.

9.7.2.1 Routing Table Overview

The IP Routing table consists of the following:

Table 9-8: IP Routing Table Layout

Destination	Prefix Length	Gateway	Interface	Metric	Status
201.201.0.0	16	192.168.0.1	0	1	Active
202.202.0.0	16	192.168.0.2	0	1	Active
203.203.0.0	16	192.168.0.3	0	1	Active
225.225.0.0	16	192.168.0.25	0	1	Inactive

9.7.2.2 Routing Table Columns

Each row of the Routing table defines a static routing rule. Traffic destined to the subnet specified in the routing rule is re-directed to the defined gateway, reachable through the specified interface.

9.7.2.2.1 Destination Column

This column defines the destination of the route rule. The destination can be a single host or a whole subnet, depending on the Prefix Length/Subnet Mask specified for this routing rule.

9.7.2.2.2 Prefix Length Column

The Prefix Length column holds the 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 that are set in the dotted-decimal format. For example, 16 is synonymous with subnet 255.255.0.0.

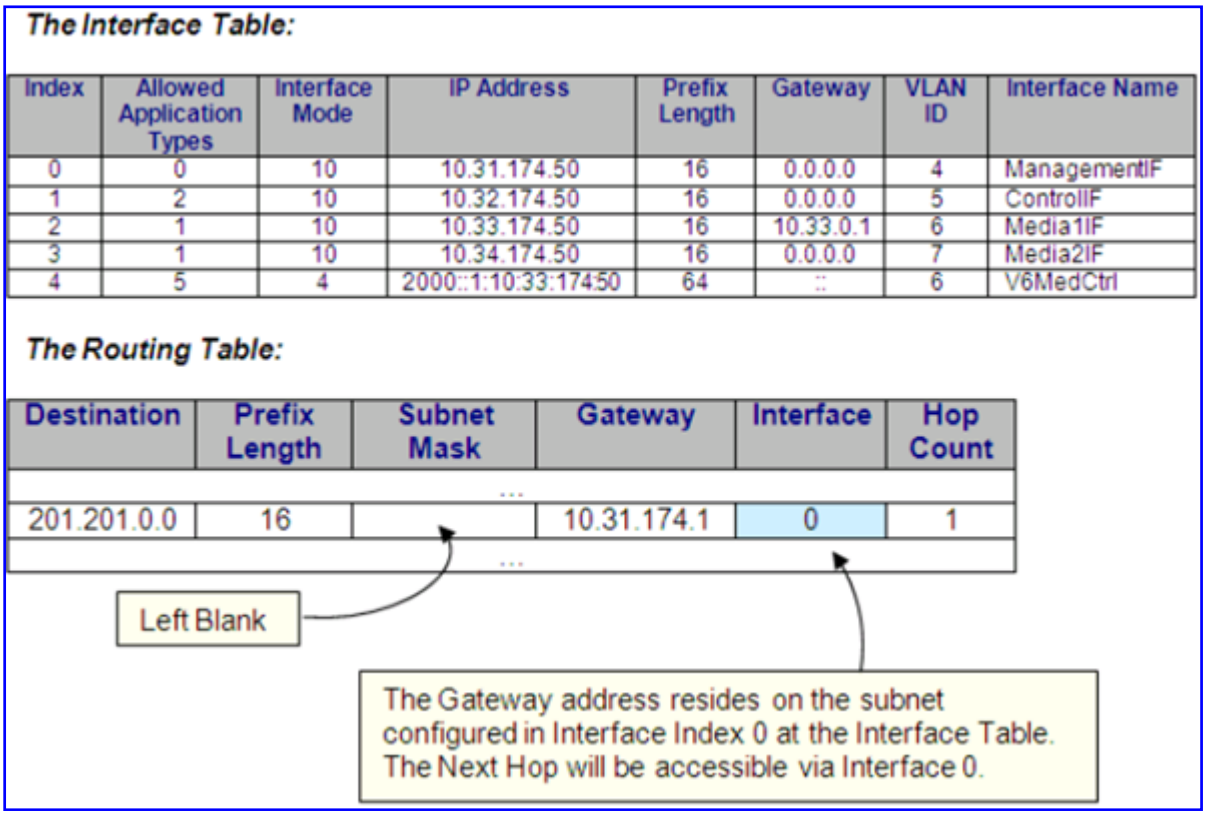
9.7.2.2.3 Gateway Column

The Gateway column defines the IP address of the next hop used for traffic destined to the subnet/host as defined in the destination/mask columns. This gateway address must be on the same subnet as the IP address of the interface configured in the Interface column.

9.7.2.2.4 Interface Column

This column defines the interface index (in the Multiple Interface table) from which the gateway address is reached.

Figure 9-3: Interface Column



9.7.2.2.5 Metric Column

The Metric column must be set to 1 for each static routing rule.

9.7.2.2.6 State Column

The State column displays the state of each static route. Possible values are "Active" and "Inactive". 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".

9.7.2.3 Routing Table Configuration Summary and Guidelines

The Routing table configurations must adhere to the following rules:

- Up to 30 different static routing rules may be defined.
- 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 must be on the same subnet as the IP address of the interfaces configured in the Interface Index column.
- The “Metric” column must be set to 1.
- Network Configuration changes are offline. The new configuration should be saved and will be available at the next startup.

9.7.2.4 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" column is unreachable from the interface specified in the "Interface" column.
- The same destination is defined in two different routing rules.
- More than 30 routing rules were defined.

Note: If a routing rule is required to access OAMP applications (for remote management, for instance) and this 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.

9.7.3 Setting Up VoIP Networking

9.7.3.1 Using the Web Interface

The Web interface is a convenient user interface for configuring the device's network configuration.

9.7.3.2 Using the ini File

When configuring the network configuration using the *ini* File, use a textual presentation of the Interface and Routing Tables, as well as some other parameters. The following shows an example of a full network configuration, consisting of **all** the parameters described in this section:

```
; VLAN related parameters:
VlanMode = 0
VlanNativeVlanId = 1
; Routing Table Configuration:
[ StaticRouteTable ]
FORMAT StaticRouteTable_Index = StaticRouteTable_InterfaceName,
StaticRouteTable_Destination, StaticRouteTable_PrefixLength, StaticRouteTable_Gateway,
StaticRouteTable_Description;
StaticRouteTable 0 = 0, 201.201.0.0, 16, 192.168.0.2, ;
StaticRouteTable 1 = 0, 202.202.0.0, 16, 192.168.0.3, ;
[ \StaticRouteTable ]

; Class Of Service parameters:
VlanNetworkServiceClassPriority = 7
VlanPremiumServiceClassMediaPriority = 6
VlanPremiumServiceClassControlPriority = 6
VlanGoldServiceClassPriority = 4
VlanBronzeServiceClassPriority = 2
NetworkServiceClassDiffServ = 48
PremiumServiceClassMediaDiffServ = 46
PremiumServiceClassControlDiffServ = 40
GoldServiceClassDiffServ = 26
BronzeServiceClassDiffServ = 10
; Application Type for applications:
EnableDNSasOAM = 1
EnableNTPasOAM = 1
; Multiple Interface Table Configuration:
[InterfaceTable]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode,
InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName;
InterfaceTable 0  = 6, 10, 192.168.85.14,  16, 192.168.0.1, 1, myAll;
```

This *ini* file shows the following:

- A Multiple Interface table with a single interface (192.168.85.14/16, OAMP, Media and Control applications are allowed) and a default gateway (192.168.0.1).
- A Routing table is configured with two routing rules, directing all traffic for subnet 201.201.0.0/16 to 192.168.0.2, and all traffic for subnet 202.202.0.0/16 to 192.168.0.3.
- VLANs are disabled; 'Native' VLAN ID is set to 1.

- Values for the Class Of Service parameters are assigned.
- The DNS application is configured to act as an OAMP application and the NTP application is configured to act as an OAMP application.

Notes:

- Lines that begin with a semicolon are considered a remark and are ignored.
- When using the *ini* file, the Multiple Interface table must have the prefix and suffix to allow the INI File parser to correctly recognize and parse the table.

9.7.3.3 Networking Configuration Examples

This section provides examples of network configurations (and their corresponding *ini* file configuration).

Example 1 - One VoIP Interface for All Applications: Multiple Interface table with a single interface for OAMP, Media and Control applications:

Table 9-9: Multiple Interface Table - Example 1

Index	Allowed Applications	Interface Mode	IP Address	Prefix Length	Default Gateway	VLAN ID	Interface Name
0	OAMP, Media & Control	IPv4	192.168.85.14	16	192.168.0.1	1	myInterface

VLANS are not required and the 'Native' VLAN ID is irrelevant. Class of Service parameters may have default values. The required routing table features two routes:

Table 9-10: Routing Table - Example 1

Destination	Prefix Length	Gateway	Interface	Metric
201.201.0.0	16	192.168.0.2	0	1
202.202.0.0	16	192.168.0.3	0	1

The DNS/NTP applications remain with their default application types.

The corresponding *ini* file configuration is shown below:

```
; Interface Table Configuration:
[InterfaceTable]
FORMAT InterfaceTable Index = InterfaceTable ApplicationTypes,
InterfaceTable InterfaceMode, InterfaceTable IPAddress,
InterfaceTable PrefixLength, InterfaceTable Gateway,
InterfaceTable VlanID, InterfaceTable InterfaceName;
InterfaceTable 0  = 6, 10, 192.168.85.14,  16, 192.168.0.1, 1,
myInterface;
[\InterfaceTable]
; Routing Table Configuration:
[ StaticRouteTable ]
FORMAT StaticRouteTable Index = StaticRouteTable InterfaceName,
StaticRouteTable Destination, StaticRouteTable PrefixLength,
StaticRouteTable Gateway, StaticRouteTable Description;
StaticRouteTable 0 = 0, 201.201.0.0, 16, 192.168.0.2, ;
StaticRouteTable 1 = 0, 202.202.0.0, 16, 192.168.0.3, ;
[ \StaticRouteTable ]
```

Example 2 - Three VoIP Interfaces, One for each Application Exclusively: the Multiple Interface table is configured with three interfaces, one exclusively for each application type: one interface for OAMP applications, one for Call Control applications, and one for RTP Media applications:

Table 9-11: Multiple Interface Table - Example2

Index	Allowed Applications	Interface Mode	IP Address	Prefix Length	Default Gateway	VLAN ID	Interface Name
0	OAMP	IPv4 Manual	192.168.85.14	16	0.0.0.0	1	ManagementIF
1	Control	IPv4 Manual	200.200.85.14	24	200.200.85.1	200	myControlIF
2	Media	IPv4 Manual	211.211.85.14	24	211.211.85.1	211	myMediaIF

VLANs are required. The 'Native' VLAN ID is the same VLAN ID as the Management interface (Index 0).

One routing rule is required to allow remote management from a host in 176.85.49.0 / 24:

Table 9-12: Routing Table - Example 2

Destination	Prefix Length	Gateway	Interface	Metric
176.85.49.0	24	192.168.0.1	0	1

All other parameters are set to their respective default values. The DNS/NTP applications are left with their default application types.

The corresponding *ini* file configuration is shown below:

```
; Interface Table Configuration:
[InterfaceTable]
FORMAT InterfaceTable Index = InterfaceTable ApplicationTypes,
InterfaceTable InterfaceMode, InterfaceTable IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable VlanID, InterfaceTable InterfaceName;
InterfaceTable 0  = 0, 10, 192.168.85.14,  16, 0.0.0.0, 1, ManagementIF;
InterfaceTable 1  = 2, 10, 200.200.85.14,  24, 200.200.85.1, 200,
myControlIF;
InterfaceTable 2  = 1, 10, 211.211.85.14,  24, 211.211.85.1, 211,
myMediaIF;
[\InterfaceTable]
; VLAN related parameters:
VlanMode = 1
VlanNativeVlanId = 1
; Routing Table Configuration:
[ StaticRouteTable ]
FORMAT StaticRouteTable Index = StaticRouteTable InterfaceName,
StaticRouteTable Destination, StaticRouteTable PrefixLength,
StaticRouteTable Gateway, StaticRouteTable Description;
StaticRouteTable 0 = 0, 176.85.49.0, 24, 192.168.0.1, ;
[ \StaticRouteTable ]
```

Example 3 - Three **I**nterfaces: one exclusively for management (OAMP applications) and two others for Call Control and RTP (Control and Media applications) :

Table 9-13: Multiple Interface Table - Example 3

Index	Allowed Applications	Interface Mode	IP Address	Prefix Length	Default Gateway	VLAN ID	Interface Name
0	OAMP	IPv4 Manual	192.168.85.14	16	192.168.0.1	1	Mgmt
1	Media & Control	IPv4 Manual	200.200.85.14	24	200.200.85.1	201	MediaCntrl1
2	Media & Control	IPv4 Manual	200.200.86.14	24	200.200.86.1	202	MediaCntrl2

VLANs are required. The 'Native' VLAN ID is the same VLAN ID as the AudioCodes Management interface (index 0).

One routing rule is required to allow remote management from a host in 176.85.49.0/24:

Table 9-14: Routing Table - Example 3

Destination	Destination Subnet Mask/Prefix Length	Gateway	Interface	Metric
176.85.49.0	24	192.168.0.10	0	1

All other parameters are set to their respective default values. The DNS/NTP applications are left with their default application types.

The corresponding *ini* file configuration is shown below:

```
; Interface Table Configuration:
[InterfaceTable]
FORMAT InterfaceTable Index = InterfaceTable ApplicationTypes,
InterfaceTable InterfaceMode, InterfaceTable IPAddress,
InterfaceTable PrefixLength, InterfaceTable Gateway,
InterfaceTable VlanID, InterfaceTable InterfaceName;
InterfaceTable 0  = 0, 10, 192.168.85.14,  16, 192.168.0.1, 1, Mgmt;
InterfaceTable 1  = 5, 10, 200.200.85.14,  24, 200.200.85.1, 201,
MediaCntrl1;
InterfaceTable 2  = 5, 10, 200.200.86.14,  24, 200.200.86.1, 202,
MediaCntrl2;

[\InterfaceTable]
; VLAN related parameters:
VlanMode = 1
VlanNativeVlanId = 1
; Routing Table Configuration:
[ StaticRouteTable ]
FORMAT StaticRouteTable Index = StaticRouteTable InterfaceName,
StaticRouteTable_Destination, StaticRouteTable_PrefixLength,
StaticRouteTable Gateway, StaticRouteTable Description;
StaticRouteTable 0 = 0, 176.85.49.0, 24, 192.168.0.1, ;
[ \StaticRouteTable ]
```

10 Configuration Parameters Reference

The device's configuration parameters, default values, and their descriptions are documented in this section.

Parameters and values enclosed in square brackets ([...]) represent the *ini* file parameters and their enumeration values; parameters not enclosed in square brackets represent their corresponding Web interface and/or EMS parameters.

Note: Some parameters are configurable only through the *ini* file.

10.1 Networking Parameters

This subsection describes the device's networking parameters.

10.1.1 Ethernet Parameters

The Ethernet parameters are described in the table below.

Table 10-1: Ethernet Parameters

Parameter	Description
EMS: Physical Configuration **[EthernetPhyConfiguration]**	Defines the Ethernet connection mode type. ▪ **[0]** = 10Base-T half-duplex (Not applicable) ▪ **[1]** = 10Base-T full-duplex ▪ **[2]** = 100Base-TX half-duplex ▪ **[3]** = 100Base-TX full-duplex ▪ **[4]** = Auto-negotiate (default) For detailed information on Ethernet interface configuration, see Ethernet Interface Configuration on page 311. **Note:** For this parameter to take effect, a device reset is required.
Web: 802.1x Mode EMS: Mode **[802.**1xMode]	Enables support for IEEE 802.1x physical port security. The device can function as an IEEE 802.1X supplicant. IEEE 802.1X is a standard for port-level security on secure Ethernet switches; when a unit is connected to a secure port, no traffic is allowed until the identity of the unit is authenticated. ▪ **[0]** Disabled (default) ▪ **[1]** EAP-MD5 = Authentication is performed using a user name and password configured by the parameters 802.1xUsername and 802.1xPassword. ▪ **[2]** Protected EAP = Authentication is performed using a user name and password configured by the parameters 802.1xUsername and 802.1xPassword. In addition, the protocol used is MSCHAPv2 over an encrypted TLS tunnel. ▪ **[3]** EAP-TLS = The device's certificate is used to establish a mutually-authenticated TLS session with the Access Server. This requires prior configuration of the server certificate and root CA (see Configuring the Certificates on page 62). The parameter 802.1xUsername is used to identify the device, however

Parameter	Description
	802.1xPassword is ignored. **Note:** The configured mode must match the configuration of the Access server (e.g., RADIUS server).
Web: 802.1x Username EMS: User Name **[802.**1xUsername]	Username for IEEE 802.1x support. The valid value is a string of up to 32 characters. The default is an empty string.
Web: 802.1x Password EMS: Password **[802.**1xPassword]	Password for IEEE 802.1x support. The valid value is a string of up to 32 characters. The default is an empty string.
Web: 802.1x Verify Peer Certificate EMS: Verify Peer Certificate **[802.**1xVerifyPeerCertificate]	Verify Peer Certificate for IEEE 802.1x support. ▪ **[0]** Disable (default) ▪ **[1]** Enable

10.1.2 Multiple Network Interfaces and VLAN Parameters

The IP network interfaces and VLAN parameters are described in the table below.

Table 10-2: IP Network Interfaces and VLAN Parameters

Parameter	Description
Web: Multiple Interface Table **EMS: IP Interface Settings**	
[InterfaceTable]	This *ini* file table parameter configures the Multiple Interface table for configuring logical IP addresses. The format of this parameter is as follows: **[InterfaceTable]** FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID, InterfaceTable_InterfaceName; **[\InterfaceTable]** 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; The above example, configures three network interfaces (OAMP, Control, and Media). **Notes:** ▪ For this *ini* file table parameter to take effect, a device reset is required. ▪ Up to 16 logical IP addresses with associated VLANs can be defined (indices 0-15). However, only up to 8 interfaces can be used for media RTP traffic (assigned to a Media Realm in the 'SIP Media Realm' table, which in turn is assigned to an IP Group). ▪ Each interface index must be unique.

Parameter	Description
	▪ Each interface must have a unique VLAN ID. ▪ Each interface must have a unique subnet. ▪ Subnets in different interfaces must not overlap (e.g., defining two interfaces with 10.0.0.1/8 and 10.50.10.1/24 is invalid). Each interface must have its own address space. ▪ Upon device start up, this 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 IPv4 interface and without VLANs. Therefore, check the Syslog for any error messages. ▪ When booting using BootP/DHCP protocols, an IP address is obtained from the server. This address is used as the OAMP address for this session, overriding the address configured using the InterfaceTable. The address specified for OAMP applications in this becomes available when booting from flash again. This enables the device to work with a temporary address for initial management and configuration while retaining the address to be used for deployment. ▪ To configure multiple IP interfaces in the Web interface and for a detailed description of the table's parameters, see "Configuring IP Interface Settings" on page 78). ▪ For a description of configuring *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
Single IP Network Parameters	
Web: IP Address EMS: Local IP Address **[LocalOAMIPAddress]**	The device's source IP address of the operations, administration, maintenance, and provisioning (OAMP) interface when operating in a single interface scenario without a Multiple Interface table. The default value is 0.0.0.0. **Note:** For this parameter to take effect, a device reset is required.
Web: Subnet Mask EMS: OAM Subnet Mask **[LocalOAMSubnetMask]**	The device's subnet mask of the OAMP interface when operating in a single interface scenario without a Multiple Interface table. The default subnet mask is 0.0.0.0. **Note:** For this parameter to take effect, a device reset is required.
Web: Default Gateway Address EMS: Local Def GW **[LocalOAMDefaultGW]**	The Default gateway of the OAMP interface when operating in a single interface scenario without a Multiple Interface table.

Parameter	Description
VLAN Parameters	
Web/EMS: VLAN Mode **[VLANMode]**	Enables the VLAN functionality. ▪ **[0]** Disable (default). ▪ **[1]** Enable = VLAN tagging (IEEE 802.1Q) is enabled. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ To operate with multiple network interfaces, VLANs must be activated. ▪ VLANs are available only when booting the device from flash. When booting using BootP/DHCP protocols, VLANs are disabled to allow easier maintenance access. In this scenario, multiple network interface capabilities are not available.
Web/EMS: Native VLAN ID **[VLANNativeVLANID]**	Defines the VLAN ID to which untagged incoming traffic is assigned. Outgoing packets sent to this VLAN are sent only with a priority tag (VLAN ID = 0). When this parameter is equal to one of the VLAN IDs in the Multiple Interface table (and VLANs are enabled), untagged incoming traffic is considered as incoming traffic for that interface. Outgoing traffic sent from this interface is sent with the priority tag (tagged with VLAN ID = 0). When this parameter is different from any value in the 'VLAN ID' column in the table, untagged incoming traffic is discarded and all outgoing traffic is tagged. **Note:** If this parameter is not set (i.e., default value is 1), but one of the interfaces has a VLAN ID configured to 1, this interface is still considered the 'Native' VLAN. If you do not wish to have a 'Native' VLAN ID and want to use VLAN ID 1, set this parameter to a value other than any VLAN ID in the table.
[EnableDNSasOAM]	Determines the application type for DNS services. ▪ **[1]** = OAMP (default) ▪ **[0]** = Control. **Note:** For this parameter to take effect, a device reset is required.
[EnableNTPasOAM]	Determines the application type for NTP services. ▪ **[1]** = OAMP (default) ▪ **[0]** = Control. **Note:** For this parameter to take effect, a device reset is required.
[VLANSendNonTaggedOnNative]	Determines whether to send non-tagged packets on the native VLAN. ▪ **[0]** = Sends priority tag packets (default). ▪ **[1]** = Sends regular packets (with no VLAN tag). **Note:** For this parameter to take effect, a device reset is required.

10.1.3 Static Routing Parameters

The static routing parameters are described in the table below.

Table 10-3: Static Routing Parameters

Parameter	Description
Static IP Routing Table	
[StaticRouteTable]	You can define up to 30 static IP routing rules for the device. These rules can be associated with IP interfaces defined in the Multiple Interface table (InterfaceTable parameter). The routing decision for sending the outgoing IP packet is based on the source subnet/VLAN. If not associated with an IP interface, the static IP rule is based on destination IP address. 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). The format of this parameter is as follows: [StaticRouteTable] FORMAT StaticRouteTable_Index = StaticRouteTable_InterfaceName, StaticRouteTable_Destination, StaticRouteTable_PrefixLength, StaticRouteTable_Gateway, StaticRouteTable_Description; [\StaticRouteTable] **Notes:** ▪ The Gateway address must be in the same subnet as configured in the 'Multiple Interface' table for (refer to "Configuring IP Interface Settings" on page 78). ▪ The StaticRouteTable_Description parameter is a string value of up to 30 characters. ▪ The metric value (next hop) is automatically set to 1.

10.1.4 Quality of Service Parameters

The Quality of Service (QoS) parameters are described in the table below.

The device allows you to specify values for Layer-2 and Layer-3 priorities by assigning values to the following service classes:

- Network Service class – network control traffic (ICMP, ARP)
- Premium Media service class – used for RTP Media traffic
- Premium Control Service class – used for Call Control traffic
- Gold Service class – used for streaming applications
- Bronze Service class – used for OAMP applications

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

Table 10-4: QoS Parameters

Parameter	Description
Layer-2 Class Of Service (CoS) Parameters (VLAN Tag Priority Field)	
Web: Network Priority EMS: Network Service Class Priority **[VLANNetworkServiceClassPriority]**	Defines the VLAN priority (IEEE 802.1p) for Network Class of Service (CoS) content. The valid range is 0 to 7. The default value is 7.
Web: Media Premium EMS: Premium Service Class Media Priority Priority **[VLANPremiumServiceClassMediaPriority]**	Defines the VLAN priority (IEEE 802.1p) for the Premium CoS content and media traffic. The valid range is 0 to 7. The default value is 6.
Web: Control Premium Priority EMS: Premium Service Class Control Priority **[VLANPremiumServiceClassControlPriority]**	Defines the VLAN priority (IEEE 802.1p) for the Premium CoS content and control traffic. The valid range is 0 to 7. The default value is 6.
Web: Gold Priority EMS: Gold Service Class Priority **[VlanGoldServiceClassPriority]**	Defines the VLAN priority (IEEE 802.1p) for the Gold CoS content. The valid range is 0 to 7. The default value is 4.
Web: Bronze Priority EMS: Bronze Service Class Priority **[VLANBronzeServiceClassPriority]**	Defines the VLAN priority (IEEE 802.1p) for the Bronze CoS content. The valid range is 0 to 7. The default value is 2.
Layer-3 Class of Service (TOS/DiffServ) Parameters	
Web: Network QoS EMS: Network Service Class Diff Serv **[NetworkServiceClassDiffServ]**	Defines the Differentiated Services (DiffServ) value for Network CoS content. The valid range is 0 to 63. The default value is 48.
Web: Media Premium QoS EMS: Premium Service Class Media Diff Serv **[PremiumServiceClassMediaDiffServ]**	Defines the DiffServ value for Premium Media CoS content (only if IPDiffServ is not set in the selected IP Profile). The valid range is 0 to 63. The default value is 46. **Note:** The value for the Premium Control DiffServ is determined by the following (according to priority): ▪ IPDiffServ value in the selected IP Profile (IPProfile parameter). ▪ PremiumServiceClassMediaDiffServ.
Web: Control Premium QoS EMS: Premium Service Class Control Diff Serv **[PremiumServiceClassControlDiffServ]**	Defines the DiffServ value for Premium Control CoS content (Call Control applications) - only if ControlIPDiffserv is not set in the selected IP Profile. The valid range is 0 to 63. The default value is 40. **Notes:** ▪ The value for the Premium Control DiffServ is determined by the following (according to priority): ✓ SigIPDiffserv value in the selected IP Profile (IPProfile parameter). ✓ PremiumServiceClassControlDiffServ. ▪ The same value must be configured for this parameter and the parameter MLPPDiffServ. ▪ Outgoing calls are tagged according to this parameter.
Web: Gold QoS EMS: Gold Service Class Diff Serv **[GoldServiceClassDiffServ]**	Defines the DiffServ value for the Gold CoS content (Streaming applications). The valid range is 0 to 63. The default value is 26.

Parameter	Description
Web: Bronze QoS EMS: Bronze Service Class Diff Serv **[BronzeServiceClassDiffServ]**	Defines the DiffServ value for the Bronze CoS content (OAMP applications). The valid range is 0 to 63. The default value is 10.

10.1.5 NAT and STUN Parameters

The Network Address Translation (NAT) and Simple Traversal of UDP through NAT (STUN) parameters are described in the table below.

Table 10-5: NAT and STUN Parameters

Parameter	Description
STUN Parameters	
Web: Enable STUN EMS: STUN Enable **[EnableSTUN]**	Determines whether Simple Traversal of UDP through NATs (STUN) is enabled. ▪ **[0]** Disable (default) ▪ **[1]** Enable When enabled, the device functions as a STUN client and communicates with a STUN server located in the public Internet. STUN is used to discover whether the device is located behind a NAT and the type of NAT. In addition, it is used to determine the IP addresses and port numbers that the NAT assigns to outgoing signaling messages (using SIP) and media streams (using RTP, RTCP and T.38). STUN works with many existing NAT types and does not require any special behavior from them. For detailed information on STUN, see STUN on page 312. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ For defining the STUN server domain name, use the parameter STUNServerDomainName.
Web: STUN Server Primary IP EMS: Primary Server IP **[STUNServerPrimaryIP]**	Defines the IP address of the primary STUN server. The valid range is the legal IP addresses. The default value is 0.0.0.0. **Note:** For this parameter to take effect, a device reset is required.
Web: STUN Server Secondary IP EMS: Secondary Server IP **[STUNServerSecondaryIP]**	Defines the IP address of the secondary STUN server. The valid range is the legal IP addresses. The default value is 0.0.0.0. **Note:** For this parameter to take effect, a device reset is required.
[STUNServerDomainName]	Defines the domain name for the Simple Traversal of User Datagram Protocol (STUN) server's address (used for retrieving all STUN servers with an SRV query). The STUN client can perform the required SRV query to resolve this domain name to an IP address and port, sort the server list, and use the servers according to the sorted list. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ Use either the STUNServerPrimaryIP or the STUNServerDomainName parameter, with priority to the first one.

Parameter	Description
NAT Parameters	
Web/EMS: NAT Traversal **[DisableNAT]**	Enables or disables the NAT mechanism. ▪ **[0]** Enable ▪ **[1]** Disable (default) **Note:** The compare operation that is performed on the IP address is enabled by default and is configured by the parameter EnableIPAddrTranslation. The compare operation that is performed on the UDP port is disabled by default and is configured by the parameter EnableUDPPortTranslation.
Web: NAT IP Address EMS: Static NAT IP Address **[StaticNatIP]**	Global (public) IP address of the device to enable static NAT between the device and the Internet. **Note:** For this parameter to take effect, a device reset is required.
EMS: Binding Life Time **[NATBindingDefaultTimeout]**	Defines the default NAT binding lifetime in seconds. STUN refreshes the binding information after this time expires. The valid range is 0 to 2,592,000. The default value is 30. **Note:** For this parameter to take effect, a device reset is required.
[EnableIPAddrTranslation]	Enables IP address translation for RTP, RTCP, and T.38 packets. ▪ **[0]** = Disable IP address translation. ▪ **[1]** = Enable IP address translation (default). ▪ **[2]** = Enable IP address translation for RTP Multiplexing (ThroughPacket™). ▪ **[3]** = Enable IP address translation for all protocols (RTP, RTCP, T.38 and RTP Multiplexing). When enabled, the device compares the source IP address of the first incoming packet to the remote IP address stated in the opening of the channel. If the two IP addresses don't match, the NAT mechanism is activated. Consequently, the remote IP address of the outgoing stream is replaced by the source IP address of the first incoming packet. **Notes:** ▪ The NAT mechanism must be enabled for this parameter to take effect (i.e., the parameter DisableNAT is set to 0). ▪ For information on RTP Multiplexing, see RTP Multiplexing (ThroughPacket) on page 310.
[EnableUDPPortTranslation]	▪ **[0]** = Disable UDP port translation (default). ▪ **[1]** = Enable UDP port translation. When enabled, the device compares the source UDP port of the first incoming packet to the remote UDP port stated in the opening of the channel. If the two UDP ports don't match, the NAT mechanism is activated. Consequently, the remote UDP port of the outgoing stream is replaced by the source UDP port of the first incoming packet. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ The NAT mechanism and the IP address translation must be enabled for this parameter to take effect (i.e., set the parameter DisableNAT to 0 and the parameter EnableIpAddrTranslation to 1).

10.1.6 NFS Parameters

The Network File Systems (NFS) configuration parameters are described in the table below.

Table 10-6: NFS Parameters

Parameter	Description
[NFSBasePort]	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. The valid range is 0 to 65535. The default is 47000.
Web: NFS Table **EMS: NFS Settings**	
[NFSServers]	This *ini* file 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). As a file system, the NFS is independent of machine types, OSs, 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. The format of this *ini* file table parameter is as follows: **[**NFSServers] FORMAT NFSServers_Index = NFSServers_HostOrIP, NFSServers_RootPath, NFSServers_NfsVersion, NFSServers_AuthType, NFSServers_UID, NFSServers_GID, NFSServers_VlanType; [\NFSServers] For example: NFSServers 1 = 101.1.13, /audio1, 3, 1, 0, 1, 1; **Notes:** ▪ You can configure up to 16 NFS file systems (where the first index is 0). ▪ To avoid terminating current calls, a row must not be deleted or modified while the device is currently accessing files on the remote NFS file system. ▪ The combination of host/IP and Root Path must be unique for each index in the table. For example, the table must include only one index entry with a Host/IP of '192.168.1.1' and Root Path of '/audio'. ▪ This parameter is applicable only if VLANs are enabled or Multiple IPs is configured. ▪ For a detailed description of the table's parameters and to configure NFS using the Web interface, see "Configuring NFS Settings" on page 59. ▪ For a description of configuring *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.1.7 DNS Parameters

The Domain name System (DNS) parameters are described in the table below.

Table 10-7: DNS Parameters

Parameter	Description
Web: DNS Primary Server IP EMS: DNS Primary Server **[DNSPriServerIP]**	The IP address of the primary DNS server. Enter the IP address in dotted-decimal notation, for example, 10.8.2.255. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ To use Fully Qualified Domain Names (FQDN) in the 'Tel to IP Routing', you must define this parameter.
Web: DNS Secondary Server IP EMS: DNS Secondary Server **[DNSSecServerIP]**	The IP address of the second DNS server. Enter the IP address in dotted-decimal notation, for example, 10.8.2.255. **Note:** For this parameter to take effect, a device reset is required.
Web: Internal DNS Table **EMS: DNS Information**	
[DNS2IP]	This *ini* file table parameter configures 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. The format of this parameter is as follows: [Dns2Ip] FORMAT Dns2Ip_Index = Dns2Ip_DomainName, Dns2Ip_FirstIpAddress, Dns2Ip_SecondIpAddress, Dns2Ip_ThirdIpAddress, Dns2Ip_FourthIpAddress; [\Dns2Ip] For example: Dns2Ip 0 = DnsName, 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4; **Notes:** ▪ This parameter can include up to 20 indices. ▪ If the internal DNS table is used, the device first attempts to resolve a domain name using this table. If the domain name isn't found, the device performs a DNS resolution using an external DNS server. ▪ To configure the internal DNS table using the Web interface and for a description of the parameters in this *ini* file table parameter, see "Configuring the Internal DNS Table" on page 87. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
Web: Internal SRV Table **EMS: DNS Information**	
[SRV2IP]	This *ini* file 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: [SRV2IP] FORMAT SRV2IP_Index = SRV2IP_InternalDomain, SRV2IP_TransportType, SRV2IP_Dns1, SRV2IP_Priority1, SRV2IP_Weight1, SRV2IP_Port1, SRV2IP_Dns2, SRV2IP_Priority2, SRV2IP_Weight2, SRV2IP_Port2, SRV2IP_Dns3, SRV2IP_Priority3,

Parameter	Description
	SRV2IP_Weight3, SRV2IP_Port3; [\SRV2IP] For example: SRV2IP 0 = SrvDomain,0,Dnsname1,1,1,500,Dnsname2,2,2,501,$$,0,0,0; **Notes**: ▪ This parameter can include up to 10 indices. ▪ If the Internal SRV table is used, the device first attempts to resolve a domain name using this table. If the domain name isn't located, the device performs an SRV resolution using an external DNS server. ▪ To configure the Internal SRV table using the Web interface and for a description of the parameters in this *ini* file table parameter, see "Configuring the Internal SRV Table" on page 88. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.1.8 DHCP Parameters

The Dynamic Host Control Protocol (DHCP) parameters are described in the table below.

Table 10-8: DHCP Parameters

Parameter	Description
Web: Enable DHCP EMS: DHCP Enable **[DHCPEnable]**	Determines whether Dynamic Host Control Protocol (DHCP) is enabled. ▪ **[0]** Disable = Disable DHCP support on the device (default). ▪ **[1]** Enable = Enable DHCP support on the device. After the device powers up, it attempts to communicate with a BootP server. If a BootP server does not respond and DHCP is enabled, then the device attempts to obtain its IP address and other networking parameters from the DHCP server. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ After you enable the DHCP server, perform the following procedure: **a.** Enable DHCP and save the configuration. **b.** Perform a cold reset using the device's hardware reset button (soft reset using the Web interface doesn't trigger the BootP/DHCP procedure and this parameter reverts to 'Disable'). ▪ Throughout the DHCP procedure, the BootP/TFTP application must be deactivated; otherwise the device receives a response from the BootP server instead of from the DHCP server. ▪ For additional information on DHCP, refer to the *Product Reference Manual*. ▪ 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 *ini* file.

Parameter	Description
EMS: DHCP Speed Factor **[DHCPSpeedFactor]**	Determines the DHCP renewal speed. ▪ **[0]** = Disable ▪ **[1]** = Normal (default) ▪ **[2]** to **[10]** = Fast 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. **Note:** For this parameter to take effect, a device reset is required.
Web: Enable DHCP Lease Renewal **[EnableDHCPLeaseRenewal]**	Enables or disables DHCP renewal support. ▪ **[0]** Disable (default) ▪ **[1]** Enable This parameter is applicable only if the parameter DHCPEnable is set to 0 for cases where booting up the device using DHCP is not desirable but renewing DHCP leasing is. When the device is powered up, it attempts to communicate with a BootP server. If there is no response and if DHCP is disabled, the device boots from flash. It then attempts to communicate with the DHCP server to renew the lease. **Note:** For this parameter to take effect, a device reset is required.
[DHCPRequestTFTPParams]	Determines whether the device includes DHCP options 66 and 67 in DHCP Option 55 (Parameter Request List) for requesting the DHCP server for TFTP provisioning parameters. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable **Note:** For this parameter to take effect, a device reset is required.

10.1.9 NTP and Daylight Saving Time Parameters

The Network Time Protocol (NTP) and daylight saving time parameters are described in the table below.

Table 10-9: NTP and Daylight Saving Time Parameters

Parameter	Description
NTP Parameters **Note:** For detailed information on Network Time Protocol (NTP), see "Simple Network Time Protocol Support" on page 315.	
Web: NTP Server IP Address EMS: Server IP Address **[NTPServerIP]**	The IP address (in dotted-decimal notation) of the NTP server. The default IP address is 0.0.0.0 (i.e., internal NTP client is disabled).
Web: NTP UTC Offset EMS: UTC Offset **[NTPServerUTCOffset]**	Defines the Universal Time Coordinate (UTC) offset (in seconds) from the NTP server. The default offset is 0. The offset range is -43200 to 43200.
Web: NTP Update Interval EMS: Update Interval **[NTPUpdateInterval]**	Defines the time interval (in seconds) that the NTP client requests for a time update. The default interval is 86400 (i.e., 24 hours). The range is 0 to 214783647. **Note:** It is not recommend to set this parameter to beyond one month (i.e., 2592000 seconds).

Parameter	Description
Daylight Saving Time Parameters	
Web: Day Light Saving Time EMS: Mode **[DayLightSavingTimeEnable]**	Determines whether to enable daylight saving time. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Web: Start Time EMS: Start **[DayLightSavingTimeStart]**	Defines the date and time when daylight saving begins. The format of the value is mo:dd:hh:mm (month, day, hour, and minutes).
Web: End Time EMS: End **[DayLightSavingTimeEnd]**	Defines the date and time when daylight saving ends. The format of the value is mo:dd:hh:mm (month, day, hour, and minutes).
Web/EMS: Offset **[DayLightSavingTimeOffset]**	Daylight saving time offset (in minutes). The valid range is 0 to 120. The default is 60.

10.2 Web and Telnet Parameters

This subsection describes the device's Web and Telnet parameters.

10.2.1 General Parameters

The general Web and Telnet parameters are described in the table below.

Table 10-10: General Web and Telnet Parameters

Parameter	Description
Web: Web and Telnet Access List Table EMS: Web Access Addresses **[WebAccessList_x]**	Defines 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). The default value is 0.0.0.0 (i.e., the device can be accessed from any IP address). For example: WebAccessList_0 = 10.13.2.66 WebAccessList_1 = 10.13.77.7 For defining the Web and Telnet Access list using the Web interface, see "Configuring Web and Telnet Access List" on page 70.

Parameter	Description
Web: Use RADIUS for Web/Telnet Login EMS: Web Use Radius Login **[WebRADIUSLogin]**	Uses RADIUS queries for Web and Telnet interface authentication. ▪ **[0]** Disable (default). ▪ **[1]** Enable. When enabled, logging in to the device's Web and Telnet embedded servers is performed through a RADIUS server. The device contacts a user-defined server and verifies the given user name and password pair against a remote database, in a secure manner. **Notes:** ▪ The parameter EnableRADIUS must be set to 1. ▪ RADIUS authentication requires HTTP basic authentication, meaning the user name and password are transmitted in clear text over the network. Therefore, it's recommended to set the parameter HTTPSOnly to 1 to force the use of HTTPS, since the transport is encrypted. ▪ If using RADIUS authentication when logging in to 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 66).

10.2.2 Web Parameters

The Web parameters are described in the table below.

Table 10-11: Web Parameters

Parameter	Description
[DisableWebTask]	Disables or enables device management through the Web interface. ▪ **[0]** = Enable Web management (default). ▪ **[1]** = Disable Web management. **Note:** For this parameter to take effect, a device reset is required.
[HTTPport]	HTTP port used for Web management (default is 80). **Note:** For this parameter to take effect, a device reset is required.
EMS: Disable WEB Config **[DisableWebConfig]**	Determines whether the entire Web interface is in read-only mode. ▪ **[0]** = Enables modifications of parameters (default). ▪ **[1]** = Web interface in read-only mode. 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'). **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ To return to read/write after you have applied read-only using this parameter (set to 1), you need to reboot your device with an ini file that doesn't include this parameter, using the BootP/TFTP Server utility (refer to the Product Reference Manual).

Parameter	Description
[ResetWebPassword]	Resets the username and password of the primary and secondary accounts to their defaults. ▪ **[0]** = Password and username retain their values (default). ▪ **[1]** = Password and username are reset (for the default username and password, see User Accounts). **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ The username and password cannot be reset from the Web interface (i.e., via AdminPage or by loading an *ini* file).
[ScenarioFileName]	Defines the file name of the Scenario file to be loaded to the device. The file name must have the *.dat extension and can be up to 47 characters. For loading a Scenario using the Web interface, see Loading a Scenario to the Device on page 48.
[WelcomeMessage]	This *ini* file table parameter configures the Welcome message that appears after a Web interface login. The format of this parameter is as follows: [WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text [\WelcomeMessage] For Example: FORMAT WelcomeMessage_Index = WelcomeMessage_Text WelcomeMessage 1 = "**********" ; WelcomeMessage 2 = "********* This is a Welcome message ***" ; WelcomeMessage 3 = "**********" ; **Notes:** ▪ Each index represents a line of text in the Welcome message box. Up to 20 indices can be defined. ▪ The configured text message must be enclosed in double quotation marks (i.e., "..."). ▪ If this parameter is not configured, no Welcome message is displayed. ▪ For a description on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.2.3 Telnet Parameters

The Telnet parameters are described in the table below.

Table 10-12: Telnet Parameters

Parameter	Description
Web: Embedded Telnet Server EMS: Server Enable **[TelnetServerEnable]**	Enables or disables the device's embedded Telnet server. Telnet is disabled by default for security. ▪ **[0]** Disable (default) ▪ **[1]** Enable Unsecured ▪ **[2]** Enable Secured (SSL) **Note:** 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 66).
Web: Telnet Server TCP Port EMS: Server Port **[TelnetServerPort]**	Defines the port number for the embedded Telnet server. The valid range is all valid port numbers. The default port is 23.
Web: Telnet Server Idle Timeout EMS: Server Idle Disconnect **[TelnetServerIdleDisconnect]**	Defines the timeout (in minutes) for disconnection of an idle Telnet session. When set to zero, idle sessions are not disconnected. The valid range is any value. The default value is 0. **Note:** For this parameter to take effect, a device reset is required.

10.3 Debugging and Diagnostics Parameters

This subsection describes the device's debugging and diagnostic parameters.

10.3.1 General Parameters

The general debugging and diagnostic parameters are described in the table below.

Table 10-13: General Debugging and Diagnostic Parameters

Parameter	Description
EMS: Enable Diagnostics **[EnableDiagnostics]**	Checks the correct functionality 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. ▪ **[0]** = Rapid and Enhanced self-test mode (default). ▪ **[1]** = Detailed self-test mode (full test of DSPs, PCM, Switch, LAN, PHY and Flash). ▪ **[2]** = A quicker version of the Detailed self-test mode (full test of DSPs, PCM, Switch, LAN, PHY, but partial test of Flash). For detailed information, refer to the *Product Reference Manual*. **Note:** For this parameter to take effect, a device reset is required.

Parameter	Description
Web: Enable LAN Watchdog **[EnableLanWatchDog]**	Determines whether the LAN Watch-Dog feature is enabled. ▪ **[0]** Disable = Disable LAN Watch-Dog (default). ▪ **[1]** Enable = Enable LAN Watch-Dog. When LAN Watch-Dog 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: ▪ 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). Lifeline is activated only if it is enabled (using the parameter LifeLineType). ▪ If the self-test fails, the device restarts to overcome internal fatal communication error. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ Enable LAN Watchdog is relevant only if the Ethernet connection is full duplex. ▪ LAN Watchdog is not applicable to MP-118.
[WatchDogStatus]	▪ **[0]** = Disable device's watch dog. ▪ **[1]** = Enable device's watch dog (default). **Note:** For this parameter to take effect, a device reset is required.
[LifeLineType]	Defines the scenario upon which the Lifeline phone is activated. The Lifeline phone is available on Port 1 of MP-11x FXS devices and on ports 1 to 4 of MP-118 FXS/FXO devices. For FXS-only devices, FXS Port 1 is connected to the POTS (Lifeline) phone as well as to the PSTN/PBX (using a splitter cable). For combined FXS and FXO devices, the FXS ports are provided with lifeline by their corresponding FXO ports connected to the PSTN/PBX (i.e. FXO Port #5 provides lifeline to FXS Port 1, FXO Port #6 provides lifeline to FXS Port 2, and so on). Upon power outage and/or network failure, PSTN connectivity is maintained for the FXS phone user. ▪ **[0]** = Lifeline is activated upon power failure (default). ▪ **[1]** = Lifeline is activated upon power failure or when the link is down (physically disconnected). ▪ **[2]** = Lifeline is activated upon power failure, when the link is down, or upon network failure (logical link disconnected). **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is applicable only to FXS interfaces. ▪ To enable Lifeline switching on network failure, the LAN watch dog must be activated (i.e., set the parameter EnableLANWatchDog to 1). ▪ For a detailed description on cabling the device for Lifeline, refer to the Installation Manual.
Web: Delay After Reset **[sec]** **[GWAppDelayTime]**	Defines the time interval (in seconds) that the device's operation is delayed after a reset. The valid range is 0 to 45. The default value is 7 seconds. **Note:** This feature helps overcome connection problems caused by some LAN routers or IP configuration parameters' modifications by a DHCP server.

10.3.2 Syslog, CDR and Debug Parameters

The Syslog, CDR and debug parameters are described in the table below.

Table 10-14: Syslog, CDR and Debug Parameters

Parameter	Description
Web: Enable Syslog EMS: Syslog enable **[EnableSyslog]**	Sends the logs and error message generated by the device to the Syslog server. ▪ **[0]** Disable = Logs and errors are not sent to the Syslog server (default). ▪ **[1]** Enable = Enables the Syslog server. **Notes:** ▪ If you enable Syslog, you must enter an IP address of the Syslog server (using the SyslogServerIP parameter). ▪ Syslog messages may increase the network traffic. ▪ To configure Syslog SIP message logging levels, use the GwDebugLevel parameter. ▪ For information on the Syslog, refer to the *Product Reference Manual*. ▪ By default, logs are also sent to the RS-232 serial port. For information on establishing a serial communications link with the device, refer to the Installation Manual.
Web/EMS: Syslog Server IP Address **[SyslogServerIP]**	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. Default IP address is 0.0.0.0. For information on Syslog, refer to the *Product Reference Manual*.
Web: Syslog Server Port EMS: Syslog Server Port Number **[SyslogServerPort]**	Defines the UDP port of the Syslog server. The valid range is 0 to 65,535. The default port is 514. For information on the Syslog, refer to the *Product Reference Manual*.
[MaxBundleSyslogLength]	The maximum size (in bytes) threshold of logged Syslog messages bundled into a single UDP packet, after which they are sent to a Syslog server. The valid value range is 0 to 1220 (where 0 indicates that no bundling occurs). The default is 1220. **Note:** This parameter is applicable only if the GWDebugLevel parameter is set to 7.
Web: CDR Server IP Address EMS: IP Address of CDR Server **[CDRSyslogServerIP]**	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. **Notes:** ▪ The CDR messages are sent to UDP port 514 (default Syslog port). ▪ This mechanism is active only when Syslog is enabled (i.e., the parameter EnableSyslog is set to 1).

Parameter	Description
Web/EMS: CDR Report Level **[CDRReportLevel]**	Determines whether Call Detail Records (CDR) are sent to the Syslog server and when they are sent. ▪ **[0]** None = CDRs are not used (default). ▪ **[1]** End Call = CDR is sent to the Syslog server at the end of each call. ▪ **[2]** Start & End Call = CDR report is sent to Syslog at the start and end of each call. ▪ **[3]** Connect & End Call = CDR report is sent to Syslog at connection and at the end of each call. ▪ **[4]** Start & End & Connect Call = CDR report is sent to Syslog at the start, at connection, and at the end of each call. **Notes:** ▪ The CDR Syslog message complies with RFC 3161 and is identified by: Facility = 17 (local1) and Severity = 6 (Informational). ▪ This mechanism is active only when Syslog is enabled (i.e., the parameter EnableSyslog is set to 1).
Web/EMS: Debug Level **[GwDebugLevel]**	Syslog debug logging level. ▪ **[0]** 0 (default) = Debug is disabled. ▪ **[1]** 1 = Flow debugging is enabled. ▪ **[5]** 5 = Flow, device interface, stack interface, session manager, and device interface expanded debugging are enabled. ▪ **[7]** 7 = This option is recommended when the device is running under "heavy" traffic. In this mode: ✓ 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. ✓ 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. 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 dispalyed using the 'acsyslog' filter instead of the regular 'syslog' filter. **Notes:** ▪ This parameter is typically set to 5 if debug traces are required. However, in cases of heavy traffic, option 7 is recommended. ▪ Options 2, 3, 4, and 6 are not recommended.
Syslog Facility Number **[SyslogFacility]**	Facility level (0 through 7) for the device's Syslog messages, according to RFC 3164. This allows you to identify Syslog messages generated by the device. This is useful, for example, if you collect the device's and other equipments' Syslog messages, at one single server. The device's Syslog messages can easily be identified and distinguished from other Syslog messages by its Facility level. Therefore, in addition to filtering Syslog messages according to IP address, the messages can be filtered according to Facility level. ▪ **[16]** = local use 0 (local0) - default ▪ **[17]** = local use 1 (local1) ▪ **[18]** = local use 2 (local2)

Parameter	Description
	▪ **[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)
Web: Activity Types to Report via Activity Log Messages **[ActivityListToLog]**	The Activity Log mechanism enables the device to send log messages (to a Syslog server) for reporting certain types of Web operations according to the below user-defined filters. ▪ **[pvc]** Parameters Value Change = Changes made on-the-fly to parameters. ▪ **[afl]** Auxiliary Files Loading = Loading of auxiliary files. ▪ **[dr]** Device Reset = Reset of device via the 'Maintenance Actions' page. **Note:** For this option to take effect, a device reset is required. ▪ **[fb]** Flash Memory Burning = Burning of files or parameters to flash (in 'Maintenance Actions' page). ▪ **[swu]** Device Software Update = cmp file loading via the Software Upgrade Wizard. ▪ **[ard]** Access to Restricted Domains = Access to restricted domains, which include the following Web pages: ✓ (1) ini parameters (AdminPage) ✓ (2) 'General Security Settings' ✓ (3) 'Configuration File' ✓ (4) 'IPSec/IKE' tables ✓ (5) 'Software Upgrade Key' ✓ (6) 'Internal Firewall' ✓ (7) 'Web Access List' ✓ (8) 'Web User Accounts' ▪ **[naa]** Non Authorized Access = Attempt to access the Web interface with a false or empty user name or password. ▪ **[spc]** Sensitive Parameters Value Change = Changes made to sensitive parameters: ✓ (1) IP Address ✓ (2) Subnet Mask ✓ (3) Default Gateway IP Address ✓ (4) ActivityListToLog ▪ **[ll]** Login and Logout = Every login and logout attempt. For example: ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc' **Note:** For the *ini* file, values must be enclosed in single quotation marks.

10.3.3 Remote Alarm Indication Parameters

The Remote Alarm Indication (RAI) parameters are described in the table below.

Table 10-15: RAI Parameters

Parameter	Description
[EnableRAI]	Enables RAI alarm generation if the device's busy endpoints exceed a user-defined threshold. ▪ **[0]** = Disable RAI (Resource Available Indication) service (default). ▪ **[1]** = RAI service enabled and an SNMP 'acBoardCallResourcesAlarm' Alarm Trap is sent.
[RAIHighThreshold]	High threshold percentage of total calls that are active (busy endpoints). When the percentage of the device's busy endpoints exceeds this high threshold, the device sends the SNMP acBoardCallResourcesAlarm alarm trap with a 'major' alarm status. The range is 0 to 100. The default value is 90. **Note:** The percentage of busy endpoints is calculated by dividing the number of busy endpoints by the total number of "enabled" endpoints.
[RAILowThreshold]	Low threshold percentage of total calls that are active (busy endpoints). When the percentage of the device's busy endpoints falls below this low threshold, the device sends an SNMP acBoardCallResourcesAlarm alarm trap with a 'cleared' alarm status. The range is 0 to 100%. The default value is 90%.
[RAILoopTime]	Time interval (in seconds) that the device periodically checks call resource availability. The valid range is 1 to 200. The default is 10.

10.3.4 Serial Parameters

The RS-232 serial parameters are described in the table below. (Serial interface is mainly used for debugging and for SMDI.)

Table 10-16: Serial Parameters

Parameter	Description
[DisableRS232]	Enables or disables the device's RS-232 port. ▪ **[0]** = RS-232 serial port is enabled (default). ▪ **[1]** = RS-232 serial port is disabled. The RS-232 serial port can be used to change the networking parameters and view error/notification messages. For information on establishing a serial communications link with the device, refer to the *Installation Manual*. **Note:** For this parameter to take effect, a device reset is required.
EMS: Baud Rate **[SerialBaudRate]**	Determines the value of the RS-232 baud rate. The valid values include the following: 1200, 2400, 9600 (default), 14400, 19200, 38400, 57600, or 115200. **Note:** For this parameter to take effect, a device reset is required.

Parameter	Description
EMS: Data **[SerialData]**	Determines the value of the RS-232 data bit. ▪ **[7]** = 7-bit. ▪ **[8]** = 8-bit (default). **Note:** For this parameter to take effect, a device reset is required.
EMS: Parity **[SerialParity]**	Determines the value of the RS-232 polarity. ▪ **[0]** = None (default). ▪ **[1]** = Odd. ▪ **[2]** = Even. **Note:** For this parameter to take effect, a device reset is required.
EMS: Stop **[SerialStop]**	Determines the value of the RS-232 stop bit. ▪ **[1]** = 1-bit (default). ▪ **[2]** = 2-bit. **Note:** For this parameter to take effect, a device reset is required.
EMS: Flow Control **[SerialFlowControl]**	Determines the value of the RS-232 flow control. ▪ **[0]** = None (default). ▪ **[1]** = Hardware. **Note:** For this parameter to take effect, a device reset is required.

10.3.5 BootP Parameters

The BootP parameters are described in the table below. The BootP parameters are special 'hidden' parameters. Once defined and saved in the device's flash memory, they are used even if they don't appear in the *ini* file.

Table 10-17: BootP Parameters

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td rowspan="2">[BootPRetries]</td><td colspan="2">Note: For this parameter to take effect, a device reset is required.
This parameter is used to:</td></tr>
<tr><td>Sets the number of BootP requests the device sends during start-up. The device stops sending BootP requests when either BootP reply is received or number of retries is reached.
▪ [1] = 1 BootP retry, 1 sec.
▪ [2] = 2 BootP retries, 3 sec.
▪ [3] = 3 BootP retries, 6 sec. (default).
▪ [4] = 10 BootP retries, 30 sec.
▪ [5] = 20 BootP retries, 60 sec.
▪ [6] = 40 BootP retries, 120 sec.
▪ [7] = 100 BootP retries, 300 sec.
▪ [15] = BootP retries indefinitely.</td><td>Sets the number of DHCP packets the device sends. If after all packets are sent there's still no reply, the device loads from flash.
▪ [1] = 4 DHCP packets
▪ [2] = 5 DHCP packets
▪ [3] = 6 DHCP packets (default)
▪ [4] = 7 DHCP packets
▪ [5] = 8 DHCP packets
▪ [6] = 9 DHCP packets
▪ [7] = 10 DHCP packets
▪ [15] = 18 DHCP packets</td></tr>
</table>

Parameter	Description
[BootPSelectiveEnable]	Enables the Selective BootP mechanism. ▪ **[1]** = Enabled. ▪ **[0]** = Disabled (default). The Selective BootP mechanism (available from Boot version 1.92) enables the device's integral BootP client to filter unsolicited BootP/DHCP replies (accepts only BootP replies that contain the text 'AUDC' in the vendor specific information field). This option is useful in environments where enterprise BootP/DHCP servers provide undesired responses to the device's BootP requests. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ When working with DHCP (i.e., the parameter DHCPEnable is set to 1), the selective BootP feature must be disabled.
[BootPDelay]	The interval between the device's startup and the first BootP/DHCP request that is issued by the device. ▪ **[1]** = 1 second (default). ▪ **[2]** = 3 second. ▪ **[3]** = 6 second. ▪ **[4]** = 30 second. ▪ **[5]** = 60 second. **Note:** For this parameter to take effect, a device reset is required.
[ExtBootPReqEnable]	▪ **[0]** = Disable (default). ▪ **[1]** = Enable extended information to be sent in BootP request. If enabled, the device uses the Vendor Specific Information field in the BootP request to provide device-related initial startup information such as blade type, current IP address, software version. For a full list of the Vendor Specific Information fields, refer to the *Product Reference Manual*. The BootP/TFTP configuration utility displays this information in the 'Client Info' column. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ This option is not available on DHCP servers.

10.4 Security Parameters

This subsection describes the device's security parameters.

10.4.1 General Parameters

The general security parameters are described in the table below.

Table 10-18: General Security Parameters

Parameter	Description
Web: Voice Menu Password **[VoiceMenuPassword]**	The password for accessing the device's voice menu for configuration and status. To activate the menu, connect a POTS telephone and dial *** (three stars) followed by the password. The default value is 12345. For detailed information on the voice menu, refer to the Installation Manual. **Note:** This parameter is applicable only to FXS interfaces.
[EnableSecureStartup]	Enables the Secure Startup mode. In this mode, downloading the ini file to the device is restricted to a URL provided in initial configuration (see the parameter IniFileURL) or using DHCP. ▪ **[0]** Disable (default). ▪ **[1]** Enable = disables TFTP and allows secure protocols such as HTTPS to fetch the device configuration. For a detailed explanation on Secure Startup, refer to the Product Reference Manual. **Note:** For this parameter to take effect, a device reset is required.
Web: Internal Firewall Parameters **EMS: Firewall Settings**	
[AccessList]	This *ini* file table parameter configures the device's access list (firewall), which defines network traffic filtering rules. For each packet received on the network interface, the table is scanned from the top down until a matching rule is found. This rule can either deny (block) or permit (allow) 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. The format of this parameter is as follows: [AccessList] FORMAT AccessList_Index = AccessList_Source_IP, AccessList_PrefixLen, AccessList_Start_Port, AccessList_End_Port, AccessList_Protocol, AccessList_Use_Specific_Interface, AccessList_Interface_ID, AccessList_Packet_Size, AccessList_Byte_Rate, AccessList_Byte_Burst, AccessList_Allow_Type; [\AccessList] For example: AccessList 10 = mgmt.customer.com, 32, 0, 80, tcp, 1, OAMP, 0, 0, 0, allow; AccessList 22 = 10.4.0.0, 16, 4000, 9000, any, 0, , 0, 0, 0, block; In the example above, Rule #10 allows traffic from the host 'mgmt.customer.com' destined to TCP ports 0 to 80 on interface OAMP (OAMP). Rule #22 blocks traffic from the subnet 10.4.xxx.yyy destined to ports 4000 to 9000.

Parameter	Description
	Notes: ▪ This parameter can include up to 50 indices. ▪ To configure the firewall using the Web interface and for a description of the parameters of this *ini* file table parameter, see "Configuring Firewall Settings" on page 89. ▪ For a description of configuring with *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.4.2 HTTPS Parameters

The Secure Hypertext Transport Protocol (HTTPS) parameters are described in the table below.

Table 10-19: HTTPS Parameters

Parameter	Description
Web: Secured Web Connection (HTTPS) EMS: HTTPS Only **[HTTPSOnly]**	Determines the protocol used to access the Web interface. ▪ **[0]** HTTP and HTTPS (default). ▪ **[1]** HTTPs Only = Unencrypted HTTP packets are blocked. **Note:** For this parameter to take effect, a device reset is required.
EMS: HTTPS Port **[HTTPSPort]**	Determines the local Secured HTTPS port of the device. The valid range is 1 to 65535 (other restrictions may apply within this range). The default port is 443. **Note:** For this parameter to take effect, a device reset is required.
EMS: HTTPS Cipher String **[HTTPSCipherString]**	Defines the Cipher string for HTTPS (in OpenSSL cipher list format). For the valid range values, refer to URL http://www.openssl.org/docs/apps/ciphers.html. The default value is '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.
Web: HTTP Authentication Mode EMS: Web Authentication Mode **[WebAuthMode]**	Determines the authentication mode for the Web interface. ▪ **[0]** Basic Mode = Basic authentication (clear text) is used (default). ▪ **[1]** Digest When Possible = Digest authentication (MD5) is used. ▪ **[2]** Basic if HTTPS, Digest if HTTP = Digest authentication (MD5) is used for HTTP, and basic authentication is used for HTTPS. **Note:** When RADIUS login is enabled (i.e., the parameter WebRADIUSLogin is set to 1), basic authentication is forced.

Parameter	Description
[HTTPSRequireClientCertificate]	Requires client certificates for HTTPS connection. The client certificate must be preloaded to the device and its matching private key must be installed on the managing PC. Time and date must be correctly set on the device for the client certificate to be verified. ▪ **[0]** = Client certificates are not required (default). ▪ **[1]** = Client certificates are required. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ For a description on implementing client certificates, see "Client Certificates" on page 65.
[HTTPSRootFileName]	Defines the name of the HTTPS trusted root certificate file to be loaded using TFTP. The file must be in base64-encoded PEM (Privacy Enhanced Mail) format. The valid range is a 47-character string. **Note:** This parameter is only applicable when the device is loaded using BootP/TFTP. For information on loading this file using the Web interface, refer to the Product Reference Manual.
[HTTPSPkeyFileName]	Defines the name of a private key file (in unencrypted PEM format) to be loaded from the TFTP server.
[HTTPSCertFileName]	Defines the name of the HTTPS server certificate file to be loaded using TFTP. The file must be in base64-encoded PEM format. The valid range is a 47-character string. **Note:** This parameter is only applicable when the device is loaded using BootP/TFTP. For information on loading this file using the Web interface, refer to the Product Reference Manual.

10.4.3 SRTP Parameters

The Secure Real-Time Transport Protocol (SRTP) parameters are described in the table below.

Table 10-20: SRTP Parameters

Parameter	Description
Web: Media Security EMS: Enable Media Security **[EnableMediaSecurity]**	Enables Secure Real-Time Transport Protocol (SRTP). ▪ **[0]** Disable = SRTP is disabled (default). ▪ **[1]** Enable = SRTP is enabled. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ SRTP reduces the number of available channels. ✓ MP-124: 18 available channels ✓ MP-118: 6 available channels ✓ MP-114: 3 available channels ✓ MP-112: No reduction

Parameter	Description
Web/EMS: Media Security Behavior **[MediaSecurityBehaviour]**	Determines the device's mode of operation when SRTP is used (i.e., when the parameter EnableMediaSecurity is set to 1). ▪ **[0]** Preferable = The device initiates encrypted calls. If negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted. (default) ▪ **[1]** 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. ▪ **[2]** Disable = The profile does not support encrypted calls (i.e., SRTP). ▪ **[3]** 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. If the remote SIP UA does not support SRTP, it ignores the crypto lines. **Notes:** ▪ Before configuring this parameter, set the EnableMediaSecurity parameter to 1. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Web: Master Key Identifier (MKI) Size EMS: Packet MKI Size **[SRTPTxPacketMKISize]**	Determines the size (in bytes) of the Master Key Identifier (MKI) in SRTP Tx packets. The range is 0 to 4. The default value is 0.
Web/EMS: SRTP offered Suites **[SRTPofferedSuites]**	Defines the offered crypto suites (cipher encryption algorithms) for SRTP. ▪ **[0]** All = All available crypto suites (default) ▪ **[1]** AES_CM_128_HMAC_SHA1_80 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 80-bit tag. ▪ **[2]** AES_CM_128_HMAC_SHA1_32 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag.
Web: Disable Authentication On Transmitted RTP Packets EMS: RTP AuthenticationDisable Tx **[RTPAuthenticationDisableTx]**	On a secured RTP session, this parameter determines whether to enable authentication on transmitted RTP packets. ▪ **[0]** Enable (default) ▪ **[1]** Disable
Web: Disable Encryption On Transmitted RTP Packets EMS: RTP EncryptionDisable Tx **[RTPEncryptionDisableTx]**	On a secured RTP session, this parameter determines whether to enable encryption on transmitted RTP packets. ▪ **[0]** Enable (default) ▪ **[1]** Disable
Web: Disable Encryption On Transmitted RTCP Packets EMS: RTCP EncryptionDisable Tx **[RTCPEncryptionDisableTx]**	On a secured RTP session, this parameter determines whether to enable encryption on transmitted RTCP packets. ▪ **[0]** Enable (default) ▪ **[1]** Disable

10.4.4 TLS Parameters

The Transport Layer Security (TLS) parameters are described in the table below.

Table 10-21: TLS Parameters

Parameter	Description
Web/EMS: TLS Version **[TLSVersion]**	Defines the supported versions of SSL/TLS (Secure Socket Layer/Transport Layer Security. ▪ **[0]** SSL 2.0-3.0 and TLS 1.0 = SSL 2.0, SSL 3.0, and TLS 1.0 are supported (default). ▪ **[1]** TLS 1.0 Only = only TLS 1.0 is used. 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. **Note:** For this parameter to take effect, a device reset is required.
Web: TLS Client Re-Handshake Interval EMS: TLS Re Handshake Interval **[TLSReHandshakeInterval]**	Defines the time interval (in minutes) between TLS Re-Handshakes initiated by the device. The interval range is 0 to 1,500 minutes. The default is 0 (i.e., no TLS Re-Handshake).
Web: TLS Mutual Authentication EMS: SIPS Require Client Certificate **[SIPSRequireClientCertificate]**	Determines the device's behavior when acting as a server for TLS connections. ▪ **[0]** Disable = The device does not request the client certificate (default). ▪ **[1]** Enable = The device requires receipt and verification of the client certificate to establish the TLS connection. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ The SIPS certificate files can be changed using the parameters HTTPSCertFileName and HTTPSRootFileName.
Web/EMS: Peer Host Name Verification Mode **[PeerHostNameVerificationMode]**	Determines whether the device verifies the Subject Name of a remote certificate when establishing TLS connections. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Server Only = Verify Subject Name only when acting as a server for the TLS connection. ▪ **[2]** Server & Client = Verify Subject Name when acting as a server or client for the TLS connection. 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. 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. 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

Parameter	Description
	terminated.
Web: TLS Client Verify Server Certificate EMS: Verify Server Certificate **[VerifyServerCertificate]**	Determines whether the device, when acting as a client for TLS connections, verifies the Server certificate. The certificate is verified with the Root CA information. ▪ **[0]** Disable (default). ▪ **[1]** Enable. **Note:** If Subject Name verification is necessary, the parameter PeerHostNameVerificationMode must be used as well.
Web/EMS: TLS Remote Subject Name **[TLSRemoteSubjectName]**	Defines the Subject Name that is compared with the name defined in the remote side certificate when establishing TLS connections. 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. The valid range is a string of up to 49 characters. **Note:** This parameter is applicable only if the parameter PeerHostNameVerificationMode is set to 1 or 2.

10.4.5 SSH Parameters

The Secure Shell (SSH) parameters are described in the table below.

Table 10-22: SSH Parameters

Parameter	Description
Web/EMS: SSH Server Enable **[SSHServerEnable]**	Enables or disables the device's embedded SSH server. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Web/EMS: SSH Server Port **[SSHServerPort]**	Defines the port number for the embedded SSH server. Range is any valid port number. The default port is 22.
[SSHAdminKey]	Determines the RSA public key for strong authentication to 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. For additional information, refer to the *Product Reference Manual*.
[SSHMaxLoginAttempts]	Defines the maximum SSH login attempts allowed for entering an incorrect password by an administrator before the SSH session is rejected. The valid range is 1 to 3. the default is 3.
[SSHEnableLastLoginMessage]	Enables or disables the message display in SSH sessions of the time and date of the last SSH login. The SSH login message displays the number of unsuccessful login attempts since the last successful login.

Parameter	Description
	▪ **[0]** Disable ▪ **[1]** Enable (default) **Note:** The last SSH login information is cleared when the device is reset.
[SSHMaxSessions]	Maximum number of simultaneous SSH sessions. The valid range is 1 to 2. The default is 2 sessions.
[SSHRequirePublicKey]	Enables or disables RSA public keys for SSH. ▪ **[0]** = RSA public keys are optional if a value is configured for the parameter SSHAdminKey (default). ▪ **[1]** = RSA public keys are mandatory. **Note:** To define the key size, use the TLSPkeySize parameter.
[TLSPkeySize]	Defines the key size (in bits) for RSA public-key encryption for newly self-signed generated keys for SSH. ▪ **[512]** ▪ **[768]** ▪ **[1024]** (default) ▪ **[2048]**

10.4.6 IPSec Parameters

The Internet Protocol security (IPSec) parameters are described in the table below.

Table 10-23: IPSec Parameters

Parameter	Description
IPSec Parameters	
Web: Enable IP Security EMS: IPSec Enable **[EnableIPSec]**	Enables or disables IPSec on the device. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** For this parameter to take effect, a device reset is required.
Web: IP Security Associations Table **EMS: IPSec SA Table**	
[IPSecSATable]	This *ini* file table parameter configures the IPSec SA table. This table allows you to configure the Internet Key Exchange (IKE) and IP Security (IPSec) protocols. You can define up to 20 IPSec peers. The format of this parameter is as follows: [IPsecSATable] FORMAT IPsecSATable_Index = IPsecSATable_RemoteEndpointAddressOrName, IPsecSATable_AuthenticationMethod, IPsecSATable_SharedKey, IPsecSATable_SourcePort, IPsecSATable_DestPort, IPsecSATable_Protocol, IPsecSATable_Phase1SaLifetimeInSec, IPsecSATable_Phase2SaLifetimeInSec, IPsecSATable_Phase2SaLifetimeInKB, IPsecSATable_DPDmode, IPsecSATable_IPsecMode, IPsecSATable_RemoteTunnelAddress, IPsecSATable_RemoteSubnetIPAddress, IPsecSATable_RemoteSubnetPrefixLength, IPsecSATable_InterfaceName;

Parameter	Description
	[\IPsecSATable] For example: IPsecSATable 1 = 0, 10.3.2.73, 0, 123456789, 0, 0, 0, 0, 28800, 3600, ; In the above example, a single IPSec/IKE peer (10.3.2.73) is configured. Pre-shared key authentication is selected, with the pre-shared key set to 123456789. In addition, a lifetime of 28800 seconds is selected for IKE and a lifetime of 3600 seconds is selected for IPSec. **Notes:** ▪ Each row in the table refers to a different IP destination. ▪ To support more than one Encryption/Authentication proposal, for each proposal specify the relevant parameters in the Format line. ▪ The proposal list must be contiguous. ▪ For a detailed description of this table and to configure the table using the Web interface, see "Configuring IP Security Associations Table" on page 95. ▪ For an explanation on using ini file table parameters, see "Configuring ini File Table Parameters" on page 194.
Web: IP Security Proposal Table **EMS: IPSec Proposal Table**	
[IPSecProposalTable]	This *ini* file table parameter configures up to four IKE proposal settings, where each proposal defines an encryption algorithm, an authentication algorithm, and a Diffie-Hellman group identifier. [IPsecProposalTable] FORMAT IPsecProposalTable_Index = IPsecProposalTable_EncryptionAlgorithm, IPsecProposalTable_AuthenticationAlgorithm, IPsecProposalTable_DHGroup; [\IPsecProposalTable] For example: IPsecProposalTable 0 = 3, 2, 1; IPsecProposalTable 1 = 2, 2, 1; In the example above, two proposals are defined: ▪ Proposal 0: AES, SHA1, DH group 2 ▪ Proposal 1: 3DES, SHA1, DH group 2 **Notes:** ▪ Each row in the table refers to a different IKE peer. ▪ To support more than one Encryption / Authentication / DH Group proposal, for each proposal specify the relevant parameters in the Format line. ▪ The proposal list must be contiguous. ▪ For a detailed description of this table and to configure the table using the Web interface, see "Configuring IP Security Proposal Table" on page 94. ▪ For an explanation on using ini file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.4.7 OCSP Parameters

The Online Certificate Status Protocol (OCSP) parameters are described in the table below.

Table 10-24: OCSP Parameters

Parameter	Description
EMS: OCSP Enable **[OCSPEnable]**	Enables or disables certificate checking using OCSP. ▪ **[0]** = Disable (default). ▪ **[1]** = Enable. For a description of OCSP, refer to the *Product Reference Manual*.
EMS: OCSP Server IP **[OCSPServerIP]**	Defines the IP address of the OCSP server. The default IP address is 0.0.0.0.
[OCSPSecondaryServerIP]	Defines the IP address (in dotted-decimal notation) of the secondary OCSP server (optional). The default IP address is 0.0.0.0.
EMS: OCSP Server Port **[OCSPServerPort]**	Defines the OCSP server's TCP port number. The default port number is 2560.
EMS: OCSP Default Response **[OCSPDefaultResponse]**	Determines the default OCSP behavior when the server cannot be contacted. ▪ **[0]** = Rejects peer certificate (default). ▪ **[1]** = Allows peer certificate.

10.5 RADIUS Parameters

The RADIUS parameters are described in the table below. For detailed information on the supported RADIUS attributes, see "Supported RADIUS Attributes" on page 304.

Table 10-25: RADIUS Parameters

Parameter	Description
Web: Enable RADIUS Access Control **[EnableRADIUS]**	Determines whether the RADIUS application is enabled. ▪ **[0]** Disable = RADIUS application is disabled (default). ▪ **[1]** Enable = RADIUS application is enabled. **Note:** For this parameter to take effect, a device reset is required.
Web: Accounting Server IP Address **[RADIUSAccServerIP]**	IP address of the RADIUS accounting server.
Web: Accounting Port **[RADIUSAccPort]**	Port of the RADIUS accounting server. The default value is 1646.
Web/EMS: RADIUS Accounting Type **[RADIUSAccountingType]**	Determines when the RADIUS accounting messages are sent to the RADIUS accounting server. ▪ **[0]** At Call Release = Sent at call release only (default). ▪ **[1]** At Connect & Release = Sent at call connect and release. ▪ **[2]** At Setup & Release = Sent at call setup and release.

Parameter	Description
Web: AAA Indications EMS: Indications **[AAAIndications]**	Determines the Authentication, Authorization and Accounting (AAA) indications. ▪ **[0]** None = No indications (default). ▪ **[3]** Accounting Only = Only accounting indications are used.
Web: Device Behavior Upon RADIUS Timeout **[BehaviorUponRadiusTimeout]**	Defines the device's response upon a RADIUS timeout. ▪ **[0]** Deny Access = Denies access. ▪ **[1]** Verify Access Locally = Checks password locally (default).
[MaxRADIUSSessions]	Number of concurrent calls that can communicate with the RADIUS server (optional). The valid range is 0 to 240. The default value is 240.
[RADIUSRetransmission]	Number of retransmission retries. The valid range is 1 to 10. The default value is 3.
[RadiusTO]	Determines the time interval (measured in seconds) the device waits for a response before a RADIUS retransmission is issued. The valid range is 1 to 30. The default value is 10.
Web: RADIUS Authentication Server IP Address **[RADIUSAuthServerIP]**	IP address of the RADIUS authentication server. **Note:** For this parameter to take effect, a device reset is required.
Web: RADIUS Authentication Server Port **[RADIUSAuthPort]**	RADIUS Authentication Server Port. **Note:** For this parameter to take effect, a device reset is required.
Web: RADIUS Shared Secret **[SharedSecret]**	'Secret' used to authenticate the device to the RADIUS server. This should be a cryptically strong password.
Web: Default Access Level **[DefaultAccessLevel]**	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 value is 200 (Security Administrator').
Web: Local RADIUS Password Cache Mode **[RadiusLocalCacheMode]**	Defines 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). ▪ **[0]** Absolute Expiry Timer = when you access a Web page, the timeout doesn't reset, instead it continues decreasing. ▪ **[1]** Reset Timer Upon Access = upon each access to a Web page, the timeout always resets (reverts to the initial value configured by RadiusLocalCacheTimeout).
Web: Local RADIUS Password Cache Timeout **[RadiusLocalCacheTimeout]**	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 0xFFFFFF. The default value is 300 (5 minutes). ▪ **[-1]** = Never expires. ▪ **[0]** = Each request requires RADIUS authentication.

Parameter	Description
Web: RADIUS VSA Vendor ID **[RadiusVSAVendorID]**	Defines the vendor ID that the device accepts when parsing a RADIUS response packet. The valid range is 0 to 0xFFFFFFFF. The default value is 5003.
Web: RADIUS VSA Access Level Attribute **[RadiusVSAAccessAttribute]**	Defines the code that indicates the access level attribute in the Vendor Specific Attributes (VSA) section of the received RADIUS packet. The valid range is 0 to 255. The default value is 35.

10.6 SNMP Parameters

The SNMP parameters are described in the table below.

Table 10-26: SNMP Parameters

Parameter	Description
Web: Enable SNMP **[DisableSNMP]**	Determines whether SNMP is enabled. ▪ **[0]** Enable = SNMP is enabled (default). ▪ **[1]** Disable = SNMP is disabled and no traps are sent.
[SNMPPort]	The device's local UDP port used for SNMP Get/Set commands. The range is 100 to 3999. The default port is 161. **Note:** For this parameter to take effect, a device reset is required.
[SNMPTrustedMGR_x]	Defines up to five IP addresses of remote trusted SNMP managers from which the SNMP agent accepts and processes SNMP Get and Set requests. **Notes:** ▪ 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. ▪ If no values are assigned to these parameters any manager can access the device. ▪ Trusted managers can work with all community strings.
EMS: Keep Alive Trap Port **[KeepAliveTrapPort]**	The port to which the keep-alive traps are sent. The valid range is 0 - 65534. The default is port 162.
[SendKeepAliveTrap]	When enabled, this parameter invokes the keep-alive trap and sends it every 9/10 of the time defined in the parameter defining NAT Binding Default Timeout. ▪ **[0]** = Disable ▪ **[1]** = Enable **Note:** For this parameter to take effect, a device reset is required.

Parameter	Description
[SNMPSysOid]	Defines the base product system OID. The default is eSNMP_AC_PRODUCT_BASE_OID_D. **Note:** For this parameter to take effect, a device reset is required.
[SNMPTrapEnterpriseOid]	Defines a 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. **Note:** For this parameter to take effect, a device reset is required.
[acUserInputAlarmDescription]	Defines the description of the input alarm.
[acUserInputAlarmSeverity]	Defines the severity of the input alarm.
[AlarmHistoryTableMaxSize]	Determines 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 100. The default value is 100. **Note:** For this parameter to take effect, a device reset is required.
[SNMPEngineIDString]	Defines the SNMP engine ID for SNMPv2/SNMPv3 agents. This is used for authenticating a user attempting to access the SNMP agent on the device. The ID can be a string of up to 36 characters. The default value 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 **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ Before setting this parameter, all SNMPv3 users must be deleted; otherwise, the parameter setting is ignored. ▪ If the supplied key does not pass validation of the 12 Hex values input or it is set with the default value, the engine ID is generated according to RFC 3411.
Web: SNMP Trap Destination Parameters **EMS: Network > SNMP Managers Table** **Note:** Up to five SNMP trap managers can be defined.	
SNMP Manager **[SNMPManagerIsUsed_x]**	Determines the validity of the parameters (IP address and port number) of the corresponding SNMP Manager used to receive SNMP traps. ▪ **[0]** (Check box cleared) = Disabled (default) ▪ **[1]** (Check box selected) = Enabled

Parameter	Description
Web: IP Address EMS: Address **[SNMPManagerTableIP_x]**	Defines the IP address of the remote host used as an SNMP Manager. The device sends SNMP traps to this IP address. Enter the IP address in dotted-decimal notation, e.g., 108.10.1.255.
Web: Trap Port EMS: Port **[SNMPManagerTrapPort_x]**	Defines the port number of the remote SNMP Manager. The device sends SNMP traps to this port. The valid SNMP trap port range is 100 to 4000. The default port is 162.
Web: Trap Enable **[SNMPManagerTrapSendingEnable_x]**	Activates or de-activates the sending of traps to the corresponding SNMP Manager. ▪ **[0]** Disable = Sending is disabled. ▪ **[1]** Enable = Sending is enabled (default).
[SNMPManagerTrapUser_x]	This parameter can be set to the name of any configured SNMPV3 user to associate with this trap destination. This determines the trap format, authentication level, and encryption level. By default, the trap is associated with the SNMP trap community string.
Web: Trap Manager Host Name **[SNMPTrapManagerHostName]**	Defines an FQDN of a remote host that is used as an SNMP manager. The resolved IP address replaces the last entry in the Trap Manager table (defined by the parameter SNMPManagerTableIP_x) and the last trap manager entry of snmpTargetAddrTable in the snmpTargetMIB. For example: 'mngr.corp.mycompany.com'. The valid range is a 99-character string.
SNMP Community String Parameters	
Community String **[SNMPReadOnlyCommunityString_x]**	Defines up to five read-only SNMP community strings (up to 19 characters each). The default string is 'public'.
Community String **[SNMPReadWriteCommunityString_x]**	Defines up to five read/write SNMP community strings (up to 19 characters each). The default string is 'private'.
Trap Community String **[SNMPTrapCommunityString]**	Community string used in traps (up to 19 characters). The default string is 'trapuser'.
Web: SNMP V3 Table **EMS: SNMP V3 Users**	
[SNMPUsers]	This *ini* file table parameter configures SNMP v3 users. The format of this parameter is as follows: [SNMPUsers] FORMAT SNMPUsers_Index = SNMPUsers_Username, SNMPUsers_AuthProtocol, SNMPUsers_PrivProtocol, SNMPUsers_AuthKey, SNMPUsers_PrivKey, SNMPUsers_Group; [\SNMPUsers] For example: SNMPUsers 1 = v3admin1, 1, 0, myauthkey, -, 1; The example above configures user 'v3admin1' with security level authNoPriv(2), authentication protocol MD5, authentication text password 'myauthkey', and ReadWriteGroup2. **Notes:**

Parameter	Description
	▪ This parameter can include up to 10 indices. ▪ For a description of this table's individual parameters and for configuring the table using the Web interface, see "Configuring SNMP V3 Users" on page 76. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194

10.7 SIP Media Realm Parameters

The SIP Media Realm parameters are described in the table below.

Table 10-27: SIP Media Realm Parameters

Parameter	Description
Web: Default CP Media Realm Name EMS: Default Realm Name **[cpDefaultMediaRealmName]**	For a description of this parameter, see Configuring Media Realms.
Web: SIP Media Realm Table **EMS: Protocol Definition > Media Realm**	
[CpMediaRealm]	This *ini* file table parameter configures the SIP 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. The format of this parameter is as follows: [CpMediaRealm] FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd; [\CpMediaRealm] For example, CpMediaRealm 1 = Mrealm1, Voice, , 6600, 20, 6790; CpMediaRealm 2 = Mrealm2, Voice, , 6800, 10, 6890; **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ This table can include up to 64 indices (where 0 is the first index). ▪ Each table index must be unique. ▪ The parameter cpDefaultRealmName can be used to define one of the Media Realms appearing in this table as the default Media Realm. If the parameter cpDefaultRealmName is not configured, then the first Media Realm appearing in this table is set as default. If this table is not configured, then the default Media Realm includes all defined media interfaces. ▪ A Media Realm can be assigned to an IP Group (in the 'IP Group' table) or an SRD (in the 'SRD' table). If different Media Realms are assigned to both an IP Group and SRD, the IP Group's Media Realm takes precedence. ▪ The parameter IPv6IF is not applicable.

Parameter	Description
	▪ For a detailed description of all the parameters included in this *ini* file table parameter and for configuring Media Realms using the Web interface, see Configuring Media Realms. ▪ For a description on configuring ini file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.8 Control Network Parameters

10.8.1 IP Group, Proxy, Registration and Authentication Parameters

The proxy server, registration and authentication SIP parameters are described in the table below.

Table 10-28: Proxy, Registration and Authentication SIP Parameters

Parameter	Description
Web: IP Group Table **EMS: Endpoints > IP Group**	
[IPGroup]	This *ini* file table parameter configures the IP Group table. The format of this parameter is as follows: [IPGroup] FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description, IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_EnableSurvivability, IPGroup_ServingIPGroup, IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable, IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm, IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_ContactName; [\IPGroup] For example: IPGroup 1 = 0, "dol gateway", 1, firstIPgroup, , 0, -1, 0, 0, -1, 0, 1, 1,; IPGroup 2 = 0, "abc server", 2, secondIPgroup, , 0, -1, 0, 0, -1, 0, 1, 2,0; IPGroup 3 = 1, "IP phones", 1, thirdIPGroup, , 0, -1, 0, 0, -1, 0, , 1, 2, ; **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ This table parameter can include up to 9 indices (where 1 is the first index). ▪ The parameters Type, EnableSurvivability, ServingIPGroup, RoutingMode, SRD, MediaRealm, ClassifyByProxySet, MaxNumOfRegUsers, InboundManSet, OutboundManSet are not applicable. ▪ For a detailed description of the *ini* file table's parameters and for configuring this table using the Web interface, see "Configuring IP Groups" on page 103. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

Parameter	Description
Web: Authentication Table **EMS: SIP Endpoints > Authentication**	
[Authentication]	This ini file table parameter defines a user name and password for authenticating each device port. The format of this parameter is as follows: [Authentication] FORMAT Authentication_Index = Authentication_UserId, Authentication_UserPassword; [\Authentication] Where, ▪ Index = port number (where 0 depicts the Port 1) ▪ UserId = User name ▪ UserPassword = Password For example: Authentication 0 = john,1325; (user name "john" with password 1325 for authenticating Port 1) Authentication 1 = lee,1552; (user name "lee" with password 1552 for authenticating Port 2) **Notes:** ▪ The parameter AuthenticationMode determines whether authentication is performed per port or for the entire device. If authentication is performed for the entire device, the configuration in this table parameter is ignored. ▪ If the user name or password is not configured, the port's phone number (configured using the parameter TrunkGroup - Endpoint Phone Number table) and global password (using the individual parameter Password) are used for authentication. ▪ Authentication is typically used for FXS interfaces, but can also be used for FXO interfaces. ▪ For configuring the Authentication table using the Web interface, see Configuring Authentication on page 153. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

Parameter	Description
Web: Account Table **EMS: SIP Endpoints > Account**	
[Account]	This *ini* file table parameter configures the Account table for registering and/or authenticating (digest) Hunt Groups (e.g., an IP-PBX) to a Serving IP Group (e.g., an Internet Telephony Service Provider - ITSP). The format of this parameter is as follows: [Account] FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup, Account_ServingIPGroup, Account_Username, Account_Password, Account_HostName, Account_Register, Account_ContactUser, Account_ApplicationType; [\Account] For example: Account 1 = 1, -1, 1, user, 1234, acl, 1, ITSP1; **Notes:** ▪ This table can include up to 10 indices (where 1 is the first index). ▪ The parameter Account_ApplicationType is not applicable. ▪ The parameter Account_ServedIPGroup is not applicable. ▪ You can define multiple table indices with the same ServedTrunkGroup but different ServingIPGroups, username, password, HostName, and ContactUser. This provides the capability for registering the same Hunt Group to several ITSP's (i.e., Serving IP Groups). ▪ For a detailed description of this table's parameters and for configuring this table using the Web interface, see "Configuring Account Table" on page 113. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
Proxy Registration Parameters	
Web: Use Default Proxy EMS: Proxy Used **[IsProxyUsed]**	Enables the use of a SIP proxy server. ▪ **[0]** No = Proxy isn't used and instead, the internal routing table is used (default). ▪ **[1]** 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 106). **Note:** If you are not using a proxy server, you must define outbound IP call routing rules in the 'Tel to IP Routing' (described in "Configuring Tel to IP Routing" on page 138).
Web/EMS: Proxy Name **[ProxyName]**	Defines the Home Proxy domain name. If specified, this name is used as the Request-URI in REGISTER, INVITE, and other SIP messages, and as the host part of the To header in INVITE messages. If not specified, the Proxy IP address is used instead. The value must be string of up to 49 characters.
Web: Redundancy Mode EMS: Proxy Redundancy Mode **[ProxyRedundancyMode]**	Determines whether the device switches back to the primary Proxy after using a redundant Proxy. ▪ **[0]** Parking = device continues working with a redundant (now active) Proxy until the next failure, after which it works

Parameter	Description
	with the next redundant Proxy (default). ▪ **[1]** Homing = device always tries to work with the primary Proxy server (i.e., switches back to the primary Proxy whenever it's available). **Note:** To use this Proxy Redundancy mechanism, you need to enable the keep-alive with Proxy option, by setting the parameter EnableProxyKeepAlive to 1 or 2.
Web: Proxy IP List Refresh Time EMS: IP List Refresh Time **[ProxyIPListRefreshTime]**	Defines the time interval (in seconds) between each Proxy IP list refresh. The range is 5 to 2,000,000. The default interval is 60.
Web: Enable Fallback to Routing Table EMS: Fallback Used **[IsFallbackUsed]**	Determines whether the device falls back to the 'Tel to IP Routing'for call routing when Proxy servers are unavailable. ▪ **[0]** Disable = Fallback is not used (default). ▪ **[1]** Enable = The 'Tel to IP Routing' is used when Proxy servers are unavailable. When the device falls back to the 'Tel to IP Routing', it continues scanning for a Proxy. When the device locates an active Proxy, it switches from internal routing back to Proxy routing. **Note:** To enable the redundant Proxies mechanism, set the parameter EnableProxyKeepAlive to 1 or 2.
Web/EMS: Prefer Routing Table **[PreferRouteTable]**	Determines whether the device's internal routing table takes precedence over a Proxy for routing calls. ▪ **[0]** No = Only a Proxy server is used to route calls (default). ▪ **[1]** Yes = The device checks the routing rules in the 'Tel to IP Routing' for a match with the Tel-to-IP call. Only if a match is not found is a Proxy used.
Web/EMS: Always Use Proxy **[AlwaysSendToProxy]**	Determines whether the device sends SIP messages and responses through a Proxy server. ▪ **[0]** Disable = Use standard SIP routing rules (default). ▪ **[1]** Enable = All SIP messages and responses are sent to the Proxy server. **Note:** This parameter is applicable only if a Proxy server is used (i.e., the parameter IsProxyUsed is set to 1).
Web: SIP ReRouting Mode EMS: SIP Re-Routing Mode **[SIPReroutingMode]**	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). ▪ **[0]** 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 (default). ▪ **[1]** 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. ▪ **[2]** Routing Table = Uses the Routing table to locate the destination and then sends a new INVITE to this destination. **Notes:** ▪ When this parameter is set to **[1]** and the INVITE sent to the Proxy fails, the device re-routes the call according to the

Parameter	Description
	Standard mode **[0].** ▪ When this parameter is set to **[2]** and the INVITE fails, the device re-routes the call according to the Standard mode **[0].** 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. ▪ When this parameter is set to **[2],** the XferPrefix parameter can be used to define different routing rules for redirect calls. ▪ This parameter is disregarded if the parameter AlwaysSendToProxy is set to 1.
Web/EMS: DNS Query Type **[DNSQueryType]**	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. ▪ **[0]** A-Record (default) ▪ **[1]** SRV ▪ **[2]** NAPTR If set to A-Record **[0],** no NAPTR or SRV queries are performed. If set to SRV **[1]** 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. If set to NAPTR **[2],** 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. 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. If a specific Transport Type is defined, a NAPTR query is not performed. **Note:** To enable NAPTR/SRV queries for Proxy servers only, use the parameter ProxyDNSQueryType.
Web: Proxy DNS Query Type **[ProxyDNSQueryType]**	Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to discover Proxy servers. ▪ **[0]** A-Record (default) ▪ **[1]** SRV ▪ **[2]** NAPTR If set to A-Record **[0],** no NAPTR or SRV queries are performed. If set to SRV **[1]** 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

Parameter	Description
	returns two domain names and the A-record queries return two IP addresses each, no additional searches are performed. If set to NAPTR **[2],** 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. If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = domain.com:5080), the device performs a regular DNS A-record query. If a specific Transport Type is defined, a NAPTR query is not performed. **Note:** When enabled, NAPTR/SRV queries are used to discover Proxy servers even if the parameter DNSQueryType is disabled.
Web/EMS: Use Gateway Name for OPTIONS **[UseGatewayNameForOptions]**	Determines whether the device uses its IP address or gateway name in keep-alive SIP OPTIONS messages. ▪ **[0]** No = Use the device's IP address in keep-alive OPTIONS messages (default). ▪ **[1]** Yes = Use 'Gateway Name' (SIPGatewayName) in keep-alive OPTIONS messages. 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).
Web/EMS: User Name **[UserName]**	User name used for Registration and Basic/Digest authentication with a Proxy/Registrar server. The default value is an empty string. **Notes:** ▪ This parameter is applicable only if single device registration is used (i.e., the parameter AuthenticationMode is set to authentication per gateway). ▪ Instead of configuring this parameter, the Authentication table can be used (see Authentication on page 153).
Web/EMS: Password **[Password]**	The password used for Basic/Digest authentication with a Proxy/Registrar server. A single password is used for all device ports. The default is 'Default_Passwd'. **Note:** Instead of configuring this parameter, the Authentication table can be used (see Authentication on page 153).
Web/EMS: Cnonce **[Cnonce]**	Cnonce string used by the SIP server and client to provide mutual authentication. The value is free format, i.e., 'Cnonce = 0a4f113b'. The default is 'Default_Cnonce'.

Parameter	Description
Web/EMS: Mutual Authentication Mode **[MutualAuthenticationMode]**	Determines the device's mode of operation when Authentication and Key Agreement (AKA) Digest Authentication is used. ▪ **[0]** Optional = Incoming requests that don't include AKA authentication information are accepted (default). ▪ **[1]** Mandatory = Incoming requests that don't include AKA authentication information are rejected.
Web/EMS: Challenge Caching Mode **[SIPChallengeCachingMode]**	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. ▪ **[0]** None = 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. (default) ▪ **[1]** INVITE Only = Challenges issued for INVITE requests are cached. This prevents a mix of REGISTER and INVITE authorizations. ▪ **[2]** Full = Caches all challenges from the proxies. **Note**: Challenge Caching is used with all proxies and not only with the active one.
Web: Proxy IP Table **EMS: Proxy IP**	
[ProxyIP]	This *ini* file 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: [ProxyIP] FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType, ProxyIp_ProxySetId; [\ProxyIP] 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; **Notes:** ▪ This parameter can include up to 32 indices (0-31). ▪ To assign various attributes (such as Proxy Load Balancing) per Proxy Set ID, use the parameter ProxySet. ▪ For configuring the Proxy Set ID table using the Web interface and for a detailed description of the parameters of this *ini* file table, see "Configuring Proxy Sets Table" on page 106. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

Parameter	Description
Web: Proxy Set Table **EMS: Proxy Set**	
[ProxySet]	This *ini* file table parameter configures the Proxy Set ID table. It is used in conjunction with the ProxyIP *ini* file table parameter, which defines the IP addresses per Proxy Set ID. The ProxySet *ini* file table 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). The format of this parameter is as follows: [ProxySet] FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD, ProxySet_ClassificationInput, ProxySet_ProxyRedundancyMode; [\ProxySet] For example: ProxySet 0 = 0, 60, 0, 0, 0, , 1; ProxySet 1 = 1, 60, 1, 0, 1, , 0; **Notes:** ▪ This table parameter can include up to 10 indices (0-9). ▪ For configuring the Proxy Set IDs and their IP addresses, use the parameter ProxyIP. ▪ The parameter ProxySet_SRD and ProxySet_ClassificationInput areis not applicable. ▪ For configuring the Proxy Set ID table using the Web interface and for a detailed description of the parameters of this *ini* file table, see "Configuring Proxy Sets Table" on page 106. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
Registrar Parameters	
Web: Enable Registration EMS: Is Register Needed **[IsRegisterNeeded]**	Enables the device to register to a Proxy/Registrar server. ▪ **[0]** Disable = The device doesn't register to Proxy/Registrar server (default). ▪ **[1]** 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). **Note:** The device sends a REGISTER request for each channel or for the entire device (according to the AuthenticationMode parameter).
Web/EMS: Registrar Name **[RegistrarName]**	Registrar domain name. If specified, the name is used as the Request-URI in REGISTER messages. If it isn't specified (default), the Registrar IP address, or Proxy name or IP address is used instead. The valid range is up to 49 characters.

Parameter	Description
Web: Registrar IP Address EMS: Registrar IP **[RegistrarIP]**	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:<5080>. **Notes:** ▪ If not specified, the REGISTER request is sent to the primary Proxy server. ▪ When a port number is specified, DNS NAPTR/SRV queries aren't performed, even if the parameter DNSQueryType is set to 1 or 2. ▪ 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. ▪ 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.
Web/EMS: Registrar Transport Type **[RegistrarTransportType]**	Determines the transport layer used for outgoing SIP dialogs initiated by the device to the Registrar. ▪ **[-1]** Not Configured (default) ▪ **[0]** UDP ▪ **[1]** TCP ▪ **[2]** TLS **Note:** When set to 'Not Configured', the value of the parameter SIPTransportType is used.
Web/EMS: Registration Time **[RegistrationTime]**	Defines the time interval (in seconds) for registering to a Proxy server. The value is used in the SIP Expires header. In addition, this parameter defines the time interval between Keep-Alive messages when the parameter EnableProxyKeepAlive is set to 2 (REGISTER). Typically, the device registers every 3,600 sec (i.e., one hour). The device resumes registration according to the parameter RegistrationTimeDivider. The valid range is 10 to 2,000,000. The default value is 180.
Web: Re-registration Timing **[%]** EMS: Time Divider **[RegistrationTimeDivider]**	Defines the re-registration timing (in percentage). The timing is a percentage of the re-register timing set by the Registrar server. The valid range is 50 to 100. The default value is 50. 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). **Note**: This parameter may be overridden if the parameter RegistrationTimeThreshold is greater than 0.
Web/EMS: Registration Retry Time **[RegistrationRetryTime]**	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. The default is 30 seconds. The range is 10 to 3600.

Parameter	Description
Web: Registration Time Threshold EMS: Time Threshold **[RegistrationTimeThreshold]**	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. The valid range is 0 to 2,000,000. The default value is 0.
Web: Re-register On INVITE Failure EMS: Register On Invite Failure **[RegisterOnInviteFailure]**	Enables immediate re-registration if no response is received for an INVITE request sent by the device. ▪ **[0]** Disable (default) ▪ **[1]** Enable When enabled, the device immediately expires its re-registration timer and commences re-registration to the same Proxy upon any of the following scenarios: ▪ The response to an INVITE request is 407 (Proxy Authentication Required) without an authentication header included. ▪ The remote SIP UA abandons a call before the device has received any provisional response (indicative of an outbound proxy server failure). ▪ 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). ▪ 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). ▪ 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).
Web: ReRegister On Connection Failure EMS: Re Register On Connection Failure **[ReRegisterOnConnectionFailure]**	Enables the device to perform SIP re-registration upon TCP/TLS connection failure. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Web: Gateway Registration Name EMS: Name **[GWRegistrationName]**	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. **Note:** 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.

Parameter	Description
Web/EMS: Authentication Mode **[AuthenticationMode]**	Determines the device's registration and authentication method. ▪ **[0]** Per Endpoint = Registration and authentication is performed separately for each endpoint. ▪ **[1]** Per Gateway = Single registration and authentication for the entire device (default). ▪ **[3]** Per FXS = Registration and authentication for FXS endpoints. Typically, authentication per endpoint is used for FXS interfaces, where each endpoint registers (and authenticates) separately with its own user name and password. Single registration and authentication (Authentication Mode = 1) is usually defined for FXO ports.
Web: Set Out-Of-Service On Registration Failure EMS: Set OOS On Registration Fail **[OOSOnRegistrationFail]**	Enables setting an endpoint or the entire device (i.e., all endpoints) to out-of-service if registration fails. ▪ **[0]** Disable (default) ▪ **[1]** Enable If the registration is per endpoint (i.e., AuthenticationMode is set to 0) or per Account (see "Configuring Hunt Group Settings" on page 126) 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. **Note:** Te out-of-service method is configured using the parameter FXSOOSBehavior.
[UnregistrationMode]	Determines whether the device performs an explicit unregister. ▪ **[0]** Disable (default) ▪ **[1]** Enable = The device sends an asterisk ("*") value in the SIP Contact header, instructing the Registrar server to remove all previous registration bindings. When enabled, the device removes SIP User Agent (UA) registration bindings in a Registrar, according to RFC 3261. Registrations are soft state and expire unless refreshed, but they can also be explicitly removed. A client can attempt to influence the expiration interval selected by the Registrar. A UA requests the immediate removal of a binding by specifying an expiration interval of "0" for that contact address in a REGISTER request. UA's should support this mechanism so that bindings can be removed before their expiration interval has passed. Use of the "*" Contact header field value allows a registering UA to remove all bindings associated with an address-of-record (AOR) without knowing their precise values. **Note:** The REGISTER-specific Contact header field value of "*" applies to all registrations, but it can only be used if the Expires header field is present with a value of "0".

Parameter	Description
Web/EMS: Add Empty Authorization Header **[EmptyAuthorizationHeader]**	Determines whether the SIP Authorization header is included in initial registration (REGISTER) requests sent by the device. ▪ **[0]** Disable (default) ▪ **[1]** Enable 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: ▪ username - set to the value of the private user identity ▪ realm - set to the domain name of the home network ▪ uri - set to the SIP URI of the domain name of the home network ▪ nonce - set to an empty value ▪ response - set to an empty value For example: `Authorization: Digest username=alice_private@home1.net, realm="home1.net", nonce="", response="e56131d19580cd833064787ecc"` **Note:** This registration header is according to the IMS 3GPP TS24.229 and PKT-SP-24.220 specifications.

Web: Add initial Route Header
[InitialRouteHeader]
	Determines whether the SIP Route header is included in initial registration or re-registration (REGISTER) requests sent by the device.
	▪ **[0]** Disable (default)
	▪ **[1]** Enable
	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:
	`Route: <sip:10.10.10.10;lr;transport=udp>`
	or
	`Route: <sip: pcscf-gm.ims.rr.com;lr;transport=udp>`

Parameter	Description
[UsePingPongKeepAlive]	Determines whether 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)” is used for reliable, connection-orientated transport types such as TCP. ▪ **[0]** Disable (default) ▪ **[1]** Enable The SIP user agent/client (i.e., device) uses a simple periodic message as a keep-alive mechanism to keep their flow to the proxy or registrar alive (used for example, to keep NAT bindings open). For connection-oriented transports such as TCP/TLS this is based on CRLF. This mechanism uses a client-to-server "ping" keep-alive and a corresponding server-to-client "pong" message. This ping-pong sequence allows the client, and optionally the server, to tell if its flow is still active and useful for SIP traffic. If the client does not receive a pong in response to its ping, it declares the flow “dead” and opens a new flow in its place. In the CRLF Keep-Alive mechanism the client periodically (defined by the PingPongKeepAliveTime parameter) sends a double-CRLF (the "ping") then waits to receive a single CRLF (the "pong"). If the client does not receive a "pong" within an appropriate amount of time, it considers the flow failed. **Note:** The device sends a CRLF message to the Proxy Set only if the Proxy Keep-Alive feature (EnableProxyKeepAlive parameter) is enabled and its transport type is set to TCP or TLS. The device first sends a SIP OPTION message to establish the TCP/TLS connection and if it receives any SIP response, it continues sending the CRLF keep-alive sequences.
[PingPongKeepAliveTime]	Defines the periodic interval (in seconds) after which a “ping” (double-CRLF) keep-alive is sent to a proxy/registrar, using the CRLF Keep-Alive mechanism. The default range is 5 to 2,000,000. The default is 120. The device uses the range of 80-100% of this user-defined value as the actual interval. For example, if the parameter value is set to 200 sec, the interval used is any random time between 160 to 200 seconds. This prevents an “avalanche” of keep-alive by multiple SIP UAs to a specific server.

10.9 General SIP Parameters

The general SIP parameters are described in the table below.

Table 10-29: General SIP Parameters

Parameter	Description
Web/EMS: Max SIP Message Length **[KB]** **[MaxSIPMessageLength]**	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. The valid value range is 1 to 50. The default is 50.
[SIPForceRport]	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. ▪ **[0]** (default) = Disabled - the device sends the SIP response to the UDP port defined in the Via header. If the Via header contains the 'rport' parameter, the response is sent to the UDP port from where the SIP request is received. ▪ **[1]** = Enabled - SIP responses are sent to the UDP port from where SIP requests are received even if the 'rport' parameter is not present in the Via header.
Web: Max Number of Active Calls EMS: Maximum Concurrent Calls **[MaxActiveCalls]**	Defines the maximum number of simultaneous active calls supported by the device. If the maximum number of calls is reached, new calls are not established. The valid range is 1 to the maximum number of supported channels. The default value is the maximum available channels (i.e., no restriction on the maximum number of calls).
Web: Number of Calls Limit **[CallLimit]**	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. ▪ **[-1]** = There is no limitation on calls for that IP Profile (default). ▪ **[0]** = Calls are rejected. **Note:** This parameter can only be configure for an IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Web: QoS statistics in SIP Release Call **[QoSStatistics]**	Determines whether the device includes call quality of service (QoS) statistics in SIP BYE and SIP 200 OK response to BYE, using the proprietary SIP header, X-RTP-Stat. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable The X-RTP-Stat header provides the following statistics: ▪ Number of received and sent voice packets ▪ Number of received and sent voice octets ▪ Received packet loss, jitter (in ms), and latency (in ms) The X-RTP-Stat header contains the following fields: ▪ PS=<voice packets sent> ▪ OS=<voice octets sent> ▪ PR=<voice packets received> ▪ OR=<voice octets received>

Parameter	Description

	▪ PL=<receive packet loss>
	▪ JI=<jitter in ms>
	▪ LA=<latency in ms>
	Below is an example of the X-RTP-Stat header in a SIP BYE message:
	`BYE sip:302@10.33.4.125 SIP/2.0`
	`Via: SIP/2.0/UDP 10.33.4.126;branch=z9hG4bKac2127550866`
	`Max-Forwards: 70`
	`From: <sip:401@10.33.4.126;user=phone>;tag=1c2113553324`
	`To: <sip:302@company.com>;tag=1c991751121`
	`Call-ID: 991750671245200001912@10.33.4.125`
	`CSeq: 1 BYE`
	`X-RTP-Stat: PS=207;OS=49680;;PR=314;OR=50240;PL=0;JI=600;LA=40;`
	`Supported: em,timer,replaces,path,resource-priority`
	`Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK ,REFER,INFO,SUBSCRIBE,UPDATE`
	`User-Agent: Sip-Gateway-/v.6.2A.008.006`
	`Reason: Q.850 ;cause=16 ;text="local"`
	`Content-Length: 0`

Web/EMS: PRACK Mode **[PrackMode]**	PRACK (Provisional Acknowledgment) mechanism mode for SIP 1xx reliable responses. ▪ **[0]** Disable ▪ **[1]** Supported (default) ▪ **[2]** Required **Notes:** ▪ The Supported and Required headers contain the '100rel' tag. ▪ The device sends PRACK messages if 180/183 responses are received with '100rel' in the Supported or Required headers.
Web/EMS: Enable Early Media **[EnableEarlyMedia]**	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. ▪ **[0]** Disable = Early Media is disabled (default). ▪ **[1]** Enable = Enables Early Media. Note that 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. **Note:** This parameter can be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122) and per Tel profile, using the TelProfile parameter (see "Configuring Tel Profiles" on page 121).
Web: 183 Message Behavior EMS: SIP 183 Behaviour **[SIP183Behaviour]**	Defines the response of the device upon receipt of a SIP 183 response. ▪ **[0]** Progress = A 183 response (without SDP) does not cause the device to play a ringback tone (default). ▪ **[1]** Alert = A 183 response is handled by the device as if a 180 Ringing response is received, and the device plays a ringback tone.
Web: Session-Expires Time EMS: Sip Session Expires **[SIPSessionExpires]**	Determines the numerical value that is sent in the Session-Expires header in the first INVITE request or response (if the call is answered). The valid range is 1 to 86,400 sec. The default is 0 (i.e., the Session-Expires header is disabled).

Parameter	Description
Web: Minimum Session-Expires EMS: Minimal Session Refresh Value **[MinSE]**	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. The valid range is 10 to 100,000. The default value is 90.
Web/EMS: Session Expires Method **[SessionExpiresMethod]**	Determines the SIP method used for session-timer updates. ▪ **[0]** Re-INVITE = Uses Re-INVITE messages for session-timer updates (default). ▪ **[1]** UPDATE = Uses UPDATE messages. **Notes:** ▪ The device can receive session-timer refreshes using both methods. ▪ The UPDATE message used for session-timer is excluded from the SDP body.
[RemoveToTagInFailureResponse]	Determines whether the device removes the 'to' header tag from final SIP failure responses to INVITE transactions. ▪ **[0]** = Do not remove tag (default). ▪ **[1]** = Remove tag.
[EnableRTCPAttribute]	Enables or disables the use of the 'rtcp' attribute in the outgoing SDP. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
EMS: Options User Part **[OPTIONSUserPart]**	Defines the user part value of the Request-URI for outgoing SIP OPTIONS requests. If no value is configured, the endpoint number is used. A special value is 'empty', indicating that no user part in the Request-URI (host part only) is used. The valid range is a 30-character string. The default value is an empty string ('').
Web: Fax Signaling Method EMS: Fax Used **[IsFaxUsed]**	Determines the SIP signaling method for establishing and transmitting a fax session after a fax is detected. ▪ **[0]** No Fax = No fax negotiation using SIP signaling. Fax transport method is according to the parameter FaxTransportMode (default). ▪ **[1]** T.38 Relay = Initiates T.38 fax relay. ▪ **[2]** G.711 Transport = Initiates fax/modem using the coder G.711 A-law/Mu-law with adaptations (see Note below). ▪ **[3]** 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/μ-law with adaptations (see the Note below). **Notes:** ▪ Fax adaptations (for options 2 and 3): ✓ 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 ▪ If the device initiates a fax session using G.711 (option 2 and possibly 3), a 'gpmd' attribute is added to the SDP in the following format: ✓ **For A-law:** 'a=gpmd:8 vbd=yes;ecan=on' ✓ **For μ-law:** 'a=gpmd:0 vbd=yes;ecan=on'

Parameter	Description
	▪ When this parameter is set to 1, 2, or 3, the parameter FaxTransportMode is ignored. ▪ 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. ▪ This parameter can also be configured per IP Profile (using the IPProfile parameter). ▪ For detailed information on fax transport methods, see "Fax/Modem Transport Modes" on page 248.
Web: SIP Transport Type EMS: Transport Type **[SIPTransportType]**	Determines the default transport layer for outgoing SIP calls initiated by the device. ▪ **[0]** UDP (default) ▪ **[1]** TCP ▪ **[2]** TLS (SIPS) **Notes:** ▪ It's recommended to use TLS for communication with a SIP Proxy and not for direct device-to-device communication. ▪ For received calls (i.e., incoming), the device accepts all these protocols. ▪ The value of this parameter is also used by the SAS application as the default transport layer for outgoing SIP calls. ▪ The device supports up to 10 simultaneous TLS sessions.
Web: SIP UDP Local Port EMS: Local SIP Port **[LocalSIPPort]**	Local UDP port for SIP messages. The valid range is 1 to 65534. The default value is 5060.
Web: SIP TCP Local Port EMS: TCP Local SIP Port **[TCPLocalSIPPort]**	Local TCP port for SIP messages. The valid range is 1 to 65535. The default value is 5060.
Web: SIP TLS Local Port EMS: TLS Local SIP Port **[TLSLocalSIPPort]**	Local TLS port for SIP messages. The valid range is 1 to 65535. The default value is 5061. **Note:** The value of this parameter must be different from the value of the parameter TCPLocalSIPPort.
Web/EMS: Enable SIPS **[EnableSIPS]**	Enables secured SIP (SIPS URI) connections over multiple hops. ▪ **[0]** Disable (default). ▪ **[1]** Enable. When the parameter SIPTransportType 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). **Note:** 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 **[EnableTCPConnectionReuse]**	Enables the reuse of the same TCP connection for all calls to the same destination. ▪ **[0]** Disable = Use a separate TCP connection for each call. ▪ **[1]** Enable = Use the same TCP connection for all calls (default).
Web/EMS: Reliable Connection Persistent Mode **[ReliableConnectionPersi**	Determines whether all TCP/TLS connections are set as persistent and therefore, not released. ▪ **[0]** = Disable (default) - all TCP connections (except those that are set to a proxy IP) are released if not used by any SIP

Parameter	Description
stentMode]	dialog\transaction. ▪ **[1]** = Enable - TCP connections to all destinations are persistent and not released unless the device reaches 70% of its maximum TCP resources. While trying to send a SIP message connection, reuse policy determines whether live connections to the specific destination are re-used. 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. **Note:** If the destination is a Proxy server, the TCP/TLS connection is persistent regardless of the settings of this parameter.
Web/EMS: TCP Timeout **[SIPTCPTimeout]**	Defines the Timer B (INVITE transaction timeout timer) and Timer F (non-INVITE transaction timeout timer), as defined in RFC 3261, when the SIP Transport Type is TCP. The valid range is 0 to 40 sec. The default value is 64*SIPT1Rtx msec.
Web: SIP Destination Port EMS: Destination Port **[SIPDestinationPort]**	SIP destination port for sending initial SIP requests. The valid range is 1 to 65534. The default port is 5060. **Note:** SIP responses are sent to the port specified in the Via header.
Web: Use user=phone in SIP URL EMS: Is User Phone **[IsUserPhone]**	Determines whether the 'user=phone' string is added to the SIP URI and SIP To header. ▪ **[0]** No = 'user=phone' string is not added. ▪ **[1]** Yes = 'user=phone' string is part of the SIP URI and SIP To header (default).
Web: Use user=phone in From Header EMS: Is User Phone In From **[IsUserPhoneInFrom]**	Determines whether the 'user=phone' string is added to the From and Contact SIP headers. ▪ **[0]** No = Doesn't add 'user=phone' string (default). ▪ **[1]** Yes = 'user=phone' string is part of the From and Contact headers.
Web: Use Tel URI for Asserted Identity **[UseTelURIForAssertedID]**	Determines the format of the URI in the P-Asserted-Identity and P-Preferred-Identity headers. ▪ **[0]** Disable = 'sip:' (default) ▪ **[1]** Enable = 'tel:'
Web: Tel to IP No Answer Timeout EMS: IP Alert Timeout **[IPAlertTimeout]**	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. The valid range is 0 to 3600. The default value is 180.
Web: Enable Remote Party ID EMS: Enable RPI Header **[EnableRPIheader]**	Enables Remote-Party-Identity headers for calling and called numbers for Tel-to-IP calls. ▪ **[0]** Disable (default). ▪ **[1]** Enable = Remote-Party-Identity headers are generated in SIP INVITE messages for both called and calling numbers.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Web: Enable History-Info Header
EMS: Enable History Info
[EnableHistoryInfo]</td><td>
Enables usage of the History-Info header.

[0] Disable (default)
[1] Enable

User Agent Client (UAC) Behavior:

Initial request: The History-Info header is equal to the Request-URI. If a PSTN Redirect number is received, it is added as an additional History-Info header with an appropriate reason.
Upon receiving the final failure response, the device copies the History-Info as is, adds the reason of the failure response to the last entry, and concatenates a new destination to it (if an additional request is sent). The order of the reasons is as follows:
<ol type="a">
Q.850 Reason
SIP Reason
SIP Response code

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:

<table>
<tr><th>SIP Reason Code</th><th>ISDN Redirecting Reason</th></tr>
<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>
</table>

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.

User Agent Server (UAS) Behavior:

The History-Info header is sent only in the final response.
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.

</td></tr>
<tr><td>Web: Use Tgrp Information
EMS: Use SIP Tgrp
[UseSIPTgrp]</td><td>
Determines whether the SIP 'tgrp' parameter is used. This SIP parameter specifies the Hunt Group to which the call belongs (according to RFC 4904). For example, the SIP message below indicates that the call belongs to Hunt Group ID 1:
INVITE sip::+16305550100;tgrp=1;trunk-context=example.com@10.1.0.3;user=phone SIP/2.0

[0] Disable (default) = The 'tgrp' parameter isn't used.
[1] Send Only = The Hunt Group number is added to the 'tgrp' parameter value in the Contact header of outgoing SIP messages. If a Hunt Group number is not associated with the call, the 'tgrp' parameter isn't included. If a 'tgrp' value is specified in incoming messages, it is ignored.
[2] Send and Receive = The functionality of outgoing SIP messages is identical to the functionality described in option 1. 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

</td></tr>
</table>

Parameter	Description
	call) contains "tgrp=<source trunk group ID>;trunk-context=<gateway IP address>". The <source trunk group ID> is the Hunt Group ID where incoming calls from Tel is received. For IP-Tel calls, the SIP 200 OK device's response contains "tgrp=<destination trunk group ID>;trunk-context=<gateway IP address>". The <destination trunk group ID> is the Hunt Group ID used for outgoing Tel calls. The <gateway IP address> in "trunk-context" can be configured using the parameter SIPGatewayName. **Note:** IP-to-Tel configuration (using the PSTNPrefix parameter) overrides the 'tgrp' parameter in incoming INVITE messages.
Web/EMS: TGRP Routing Precedence **[TGRProutingPrecedence]**	Determines the precedence method for routing IP-to-Tel calls - according to the 'IP to Hunt Group Routing Table' or according to the SIP 'tgrp' parameter. ▪ **[0]** (default) = IP-to-Tel routing is determined by the 'IP to Hunt Group Routing Table' (PSTNPrefix parameter). If a matching rule is not found in this table, the device uses the Hunt Group parameters for routing the call. ▪ **[1]** = 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 Hunt Group number is not defined, then the 'IP to Hunt Group Routing Table' is used for routing the call. Below is an example of an INVITE Request-URI with the 'tgrp' parameter, indicating that the IP call should be routed to Hunt Group 7: INVITE sip:200;tgrp=7;trunk-context=example.com@10.33.2.68;user=phone SIP/2.0 **Notes:** ▪ For enabling routing based on the 'tgrp' parameter, the UseSIPTgrp parameter must be set to 2. ▪ For IP-to-Tel routing based on the 'dtg' parameter (instead of the 'tgrp' parameter), use the parameter UseBroadsoftDTG.
[UseBroadsoftDTG]	Determines whether the device uses the 'dtg' parameter for routing IP-to-Tel calls to a specific Hunt Group. ▪ **[0]** Disable (default) ▪ **[1]** Enable 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 Hunt 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). For example, the received SIP message below routes the call to Hunt Group ID 56: INVITE sip:123456@192.168.1.2;dtg=56;user=phone SIP/2.0 **Note:** If the Hunt Group is not found based on the 'dtg' parameter, the 'IP to Hunt Group Routing Table' is used instead for routing the call to the appropriate Hunt Group.
Web/EMS: Enable GRUU **[EnableGRUU]**	Determines whether the Globally Routable User Agent URIs (GRUU) mechanism is used, according to RFC 5627. This is used for obtaining a GRUU from a registrar and for communicating a GRUU to a peer within a dialog. ▪ **[0]** Disable (default)

Parameter	Description

	▪ **[1]** Enable
	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:
	`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)`
	The Refer-To header needs to contain a URI that user C can use to place a call to user B. This call needs to route to the specific UA instance that user B is using to talk to user A. User B should provide user A with a URI that has to be usable by anyone. It needs to be a GRUU.
	▪ 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:
	✓ If the REGISTER is per the device's client (endpoint), it is the MAC address concatenated with the phone number of the client.
	✓ If the REGISTER is per device, it is the MAC address only.
	✓ When using TP, "User Info" can be used for registering per endpoint. Thus, each endpoint can get a unique id – its phone number. The globally unique ID in TP is the MAC address concatenated with the phone number of the endpoint.
	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.
	▪ 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.

EMS: Is CISCO Sce Mode **[IsCiscoSCEMode]**	Determines whether a Cisco gateway exists at the remote side. ▪ **[0]** = No Cisco gateway exists at the remote side (default). ▪ **[1]** = A Cisco gateway exists at the remote side. When a Cisco gateway exists at the remote side, the device must set the value of the 'annexb' parameter of the fmtp attribute in the SDP to '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. **Note:** The IsCiscoSCEMode parameter is applicable only when the selected coder is G.729.

Parameter	Description

Web: User-Agent Information
EMS: User Agent Display Info
[UserAgentDisplayInfo]
	Defines the string that is used in the SIP User-Agent and Server response headers. When configured, the string '<UserAgentDisplayInfo value>/software version' is used, for example:
	`User-Agent: myproduct/v.6.00.010.006`
	If not configured, the default string, '<AudioCodes product-name>/software version' is used, for example:
	`User-Agent: Audiocodes-Sip-Gateway-MediaPack/v.6.00.010.006`
	The maximum string length is 50 characters.
	Note: The software version number and preceding forward slash (/) cannot be modified. Therefore, it is recommended not to include a forward slash in the parameter's value (to avoid two forward slashes in the SIP header, which may cause problems).

Web/EMS: SDP Session Owner **[SIPSDPSessionOwner]**	Determines the value of the Owner line ('o' field) in outgoing SDP messages. The valid range is a string of up to 39 characters. The default value is 'AudiocodesGW'. For example: `o=AudiocodesGW 1145023829 1145023705 IN IP4 10.33.4.126`
[EnableSDPVersionNegotiation]	This feature enables the flexibility of ignoring a new SDP re-offer (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. 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. ▪ **[0]** Disable = The device negotiates any new SDP re-offer, regardless of the origin field (default). ▪ **[1]** Enable = The device negotiates only an SDP re-offer with an incremented origin field.
Web/EMS: Subject **[SIPSubject]**	Defines the value of the Subject header in outgoing INVITE messages. If not specified, the Subject header isn't included (default). The maximum length is up to 50 characters.
Web: Multiple Packetization Time Format EMS: Multi Ptime Format **[MultiPtimeFormat]**	Determines whether the 'mptime' attribute is included in the outgoing SDP. ▪ **[0]** None = Disabled (default) ▪ **[1]** PacketCable = includes the 'mptime' attribute in the outgoing SDP - PacketCable-defined format 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.

Parameter	Description
EMS: Enable P Time **[EnablePtime]**	Determines whether the 'ptime' attribute is included in the SDP. ▪ **[0]** = Remove the 'ptime' attribute from SDP. ▪ **[1]** = Include the 'ptime' attribute in SDP (default).
Web/EMS: 3xx Behavior **[3xxBehavior]**	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, Branch, To, and From tags) or change them in the new initiated INVITE. ▪ **[0]** Forward = Use different call identifiers for a redirected INVITE message (default). ▪ **[1]** Redirect = Use the same call identifiers.
Web/EMS: Enable P-Charging Vector **[EnablePChargingVector]**	Enables the inclusion of the P-Charging-Vector header to all outgoing INVITE messages. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Web/EMS: Retry-After Time **[RetryAfterTime]**	Determines the time (in seconds) used in the Retry-After header when a 503 (Service Unavailable) response is generated by the device. The time range is 0 to 3,600. The default value is 0.
Web/EMS: Fake Retry After **[sec]** **[FakeRetryAfter]**	Determines whether the device, upon receipt of a SIP 503 response without a Retry-After header, behaves as if the 503 response included a Retry-After header and with the period (in seconds) specified by this parameter. ▪ **[0]** Disable ▪ Any positive value (in seconds) for defining the period When enabled, this feature allows the device to operate with Proxy servers that do not include the Retry-After SIP header in SIP 503 (Service Unavailable) responses to indicate an unavailable service. The Retry-After header is used with the 503 (Service Unavailable) response to indicate how long the service is expected to be unavailable to the requesting SIP client. The device maintains a list of available proxies, by using the Keep-Alive mechanism. The device checks the availability of proxies by sending SIP OPTIONS every keep-alive timeout to all proxies. If the device receives a SIP 503 response to an INVITE, it also marks that the proxy is out of service for the defined "Retry-After" period.
Web/EMS: Enable P-Associated-URI Header **[EnablePAssociatedURIHeader]**	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. ▪ **[0]** Disable (default). ▪ **[1]** Enable. **Note:** P-Associated-URIs in registration responses is handled only if the device is registered per endpoint.
Web/EMS: Source Number Preference **[SourceNumberPreference]**	Determines the SIP header used for the source number in incoming INVITE messages. ▪ **''** = (empty string) Use the device's internal logic for header preference (default). The logic for filling the calling party parameters is as follows: the SIP header is selected first from which the calling party parameters are obtained: first priority is P-Asserted-Identity, second is Remote-Party-ID, and third is the From header. Once a URL is selected, all the calling party parameters are set from this

Parameter	Description
	header. If P-Asserted-Identity is selected, the Privacy header is checked and if the Privacy is set to 'id', the calling number is assumed restricted. ▪ **'FROM'** = Use the source number received in the From header.
[SelectSourceHeaderForCalledNumber]	Determines the SIP header used for obtaining the called number (destination) for IP-to-Tel calls. ▪ **[0]** Request-URI header (default) = Obtains the destination number from the user part of the Request-URI. ▪ **[1]** To header = Obtains the destination number from the user part of the To header. ▪ **[2]** P-Called-Party-ID header = Obtains the destination number from the P-Called-Party-ID header.
Web/EMS: Forking Handling Mode **[ForkingHandlingMode]**	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 to-tag than the previous 18x response. Those responses usually are generated by Proxy/Application servers that perform call forking, sending the device's originating INVITE to several destinations, using the same CallID. ▪ **[0]** Parallel handling = If SIP 18x with SDP is received, the device opens a voice stream according to the received SDP and disregards any 18x forking responses (with or without SDP) received thereafter. If the first response is 180 without SDP, the device responds according to the PlayRBTone2TEL parameter and disregards the subsequent forking 18x responses. (default) ▪ **[1]** Sequential handling = If 18x with SDP is received, the device 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. **Note:** 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.
Web: Forking Timeout **[ForkingTimeOut]**	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. The number of supported forking calls per channel is 4. In other words, for an INVITE message, the device can receive up to 4 forking responses from the Proxy server. The valid range is 0 to 30. The default is 30.
Web/EMS: Enable Reason Header **[EnableReasonHeader]**	Enables or disables the usage of the SIP Reason header. ▪ **[0]** Disable ▪ **[1]** Enable (default)

Parameter	Description
Web/EMS: Gateway Name **[SIPGatewayName]**	Assigns a name to the device (e.g., 'device123.com'). Ensure that the name you choose is the one with which the Proxy is configured to identify the device. **Note:** If specified, the device 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).
[ZeroSDPHandling]	Determines the device's response to an incoming SDP that includes an IP address of 0.0.0.0 in the SDP's Connection Information field (i.e., "c=IN IP4 0.0.0.0"). ▪ **[0]** = Sets the IP address of the outgoing SDP's c= field to 0.0.0.0 (default). ▪ **[1]** = Sets the IP address of the outgoing SDP c= field to the IP address of the device. If the incoming SDP doesn't contain the "a=inactive" line, the returned SDP contains the "a=recvonly" line.
Web/EMS: Enable Delayed Offer **[EnableDelayedOffer]**	Determines whether the device sends the initial INVITE message with or without an SDP. Sending the first INVITE without SDP is typically done by clients for obtaining the far-end's full list of capabilities before sending their own offer. (An alternative method for obtaining the list of supported capabilities is by using SIP OPTIONS, which is not supported by every SIP agent.) ▪ **[0]** Disable = The device sends the initial INVITE message with an SDP (default). ▪ **[1]** Enable = The device sends the initial INVITE message without an SDP.
Web/EMS: Enable Contact Restriction **[EnableContactRestriction]**	Determines whether the device sets the Contact header of outgoing INVITE requests to 'anonymous' for restricted calls. ▪ **[0]** Disable (default) ▪ **[1]** Enable
[AnonymousMode]	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. ▪ **[0]** = (default) If the device receives a call from the Tel with blocked caller ID, it sends an INVITE with From: "anonymous"<anonymous@anonymous.invalid> ▪ **[1]** = The device's IP address is used as the URI host part instead of "anonymous.invalid". 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" <anonymous@anonymous.invalid>. 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.
EMS: P Asserted User Name **[PAssertedUserName]**	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). The default value is null.

Parameter	Description
EMS: Use URL In Refer To Header **[UseAORInReferToHeader]**	Defines the source for the SIP URI set in the Refer-To header of outgoing REFER messages. ▪ **[0]** = Use SIP URI from Contact header of the initial call (default). ▪ **[1]** = Use SIP URI from To/From header of the initial call.
Web: Enable User-Information Usage **[EnableUserInfoUsage]**	Enables or disables 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 170.) ▪ **[0]** Disable (default). ▪ **[1]** Enable
[HandleReasonHeader]	Determines whether the device uses the value of the incoming SIP Reason header for Release Reason mapping. ▪ **[0]** Disregard Reason header in incoming SIP messages. ▪ **[1]** Use the Reason header value for Release Reason mapping (default).
[EnableSilenceSuppInSDP]	Determines the device's behavior upon receipt of SIP Re-INVITE messages that include the SDP's 'silencesupp:off' attribute. ▪ **[0]** = Disregard the 'silecesupp' attribute (default). ▪ **[1]** = Handle incoming Re-INVITE messages that include the 'silencesupp:off' attribute in the SDP as a request to switch to the Voice-Band-Data (VBD) mode. In addition, the device includes the attribute 'a=silencesupp:off' in its SDP offer. **Note:** This parameter is applicable only if the G.711 coder is used.
[EnableRport]	Enables or disables the usage of the 'rport' parameter in the Via header. ▪ **[0]** = Enabled. ▪ **[1]** = Disabled (default). 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. If the Via header doesn't include the 'rport' parameter, the destination port of the response is obtained from the host part of the Via header. If the Via header includes the 'rport' parameter without a port value, the destination port of the response is the source port of the incoming request. 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' parmeter.
EMS: X Channel Header **[XChannelHeader]**	Determines whether the SIP X-Channel header is added to SIP messages for providing information on the physical channel on which the call is received or placed. ▪ **[0]** Disable = X-Channel header is not used (default). ▪ **[1]** Enable = X-Channel header is generated by the device and sent in INVITE messages and 180, 183, and 200 OK SIP responses. The header includes the channel, and the device's IP address. For example, 'x-channel: DS/DS1-1/8;IP=192.168.13.1', where: ✓ 'DS/DS-1' is a constant string ✓ '1' is a constant string ✓ '8' is the channel (port) ✓ 'IP=192.168.13.1' is the device's IP address

Parameter	Description
Web/EMS: Progress Indicator to IP **[ProgressIndicator2IP]**	For Analog (FXS/FXO) interfaces: ▪ **[-1**] Not Configured (default) = Default values are used. The default for FXO interfaces is 1; The default for FXS interfaces is 0. ▪ **[0]** 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). ▪ **[1]** PI = 1, **[8]** 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 other network announcements). **Note:** This parameter can also be configured per IP Profile (using the IPProfile parameter) and Tel Profile (using the TelProfile parameter).
[EnableRekeyAfter181]	Enables the device to send a Re-INVITE with a new (different) SRTP key (in the SDP) upon receipt of a SIP 181 response ("call is being forwarded"). ▪ **[0]** = Disable (default) ▪ **[1]** = Enable **Note:** This parameter is applicable only if SRTP is used.
[NumberOfActiveDialogs]	Defines the maximum number of active SIP dialogs that are not call related (i.e., REGISTER and SUBSCRIBE). This parameter is used to control the Registration/Subscription rate. The valid range is 1 to 5. The default value is 5.
Web/EMS: Default Release Cause **[DefaultReleaseCause]**	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. The default release cause is NO_ROUTE_TO_DESTINATION (3). Other common values include NO_CIRCUIT_AVAILABLE (34), DESTINATION_OUT_OF_ORDER (27), etc. **Notes:** ▪ 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). ▪ For an explanation on mapping PSTN release causes to SIP responses, see Mapping PSTN Release Cause to SIP Response on page 278. ▪ For a list of SIP responses-Q.931 release cause mapping, see Release Reason Mapping.
Web: Enable Microsoft Extension **[EnableMicrosofExt]**	Modifies the called 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 party. ▪ **[0]** Disable (default). ▪ **[1]** Enable. For example, if a calling party makes a call to telephone number 622125519100 Ext. 104, the device receives the SIP INVITE (from Microsoft's application) with the URI user part as INVITE sip:622125519100;ext=104@10.1.1.10 (or INVITE tel:622125519100;ext=104). If the parameter EnableMicrosofExt is enabled, the device modifies the called number by adding an "e" as the

Parameter	Description
	prefix, removing the "ext=" parameter, and adding the extension number as the suffix (e.g., **e**622125519100**104**). Once modified, the device can then manipulate the number further, using the Number Manipulation tables (see "Number Manipulation and Routing Parameters" on page 474) 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. ▪ **[0]** = 'tel:' (default) ▪ **[1]** = 'sip:'
[TimeoutBetween100And18x]	Defines the timeout (in msec) between receiving a 100 Trying response and a subsequent 18x response. If a 18x response is not received before this timer expires, the call is disconnected. The valid range is 0 to 32,000. The default value is 0 (i.e., no timeout).
[IgnoreRemoteSDPMKI]	Determines whether the device ignores the Master Key Identifier (MKI) if present in the SDP received from the remote side. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Web: Comfort Noise Generation Negotiation EMS: Comfort Noise Generation **[ComfortNoiseNegotiation]**	Enables negotiation and usage of Comfort Noise (CN). ▪ **[0]** Disable ▪ **[1]** Enable (default) 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. To determine CNG support, the device uses the ComfortNoiseNegotiation parameter and the codec's SCE (silence suppression setting) using the CodersGroup parameter. If the ComfortNoiseNegotiation parameter is enabled, then the following occurs: ▪ 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. ▪ If the device is the receiver and the remote SIP UA does not send a "CN" in the SDP, then no CNG occurs. If the remote side sends a "CN", the device attempts to be compatible with the remote side and even if the codec's SCE is disabled, CNG occurs. 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.
Web/EMS: First Call Ringback Tone ID **[FirstCallRBTId]**	Determines 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). The valid range is -1 to 1,000. The default value is -1 (i.e., play standard Ringback tone).

Parameter	Description
	Notes: ▪ It is assumed that all Ringback tones are defined in sequence in the CPT file. ▪ In case of an MLPP call, the device uses the value of 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).
Web: Reanswer Time EMS: Regret Time **[RegretTime]**	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. The valid range is 0 to 255 (in seconds). The default value is 0.
Web: Enable Reanswering Info **[EnableReansweringINFO]**	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. ▪ **[0]** Disable (default) ▪ **[1]** Enable 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 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). The INFO message format is as follows: 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: <sip:+551137077803@ims.acme.com.br:5080;user=phone>;tag=008277765 To: <sip:notavailable@unknown.invalid>;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 **Notes:** ▪ This parameter is applicable only if the parameter RegretTime is configured. ▪ This parameter is applicable only to FXS interfaces.
Web: RTP Only Mode **[RTPOnlyMode]**	Enables the device to start sending and/or receiving 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). ▪ **[0]** Disable (default) ▪ **[1]** Transmit & Receive = Send and receive RTP

Parameter	Description
	▪ **[2]** Transmit Only= Send RTP only ▪ **[3]** Receive Only= Receive RTP only **Notes:** ▪ To configure the RTP Only mode per trunk, use the RTPOnlyModeForTrunk_ID parameter. ▪ If per trunk configuration (using the RTPOnlyModeForTrunk_ID parameter) is set to a value other than the default, the RTPOnlyMode parameter value is ignored.
Web/EMS: SIT Q850 Cause **[SITQ850Cause]**	Determines 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. The valid range is 0 to 127. The default value is 34. **Notes:** ▪ For mapping specific SIT tones, you can use the SITQ850CauseForNC, SITQ850CauseForIC, SITQ850CauseForVC, and SITQ850CauseForRO parameters. ▪ This parameter is applicable only to FXO interfaces.
Web/EMS: SIT Q850 Cause For NC **[SITQ850CauseForNC]**	Determines 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 Tel for IP-to-Tel calls. The valid range is 0 to 127. The default value is 34. **Notes:** ▪ When not configured (i.e., default), the SITQ850Cause parameter is used. ▪ This parameter is applicable only to FXO interfaces.
Web/EMS: SIT Q850 Cause For IC **[SITQ850CauseForIC]**	Determines 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 Tel for IP-to-Tel calls. The valid range is 0 to 127. The default value is -1 (not configured). **Notes:** ▪ When not configured (i.e., default), the SITQ850Cause parameter is used. ▪ This parameter is applicable only to FXO interfaces.
Web/EMS: SIT Q850 Cause For VC **[SITQ850CauseForVC]**	Determines 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 Tel for IP-to-Tel calls. The valid range is 0 to 127. The default value is -1 (not configured). **Notes:** ▪ When not configured (i.e., default), the SITQ850Cause parameter is used. ▪ This parameter is applicable only to FXO interfaces.
Web/EMS: SIT Q850 Cause For RO **[SITQ850CauseForRO]**	Determines 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 Tel for IP-to-Tel calls. The valid range is 0 to 127. The default value is -1 (not configured). **Notes:** ▪ When not configured (i.e., default), the SITQ850Cause parameter is

Parameter	Description
	used. ▪ This parameter is applicable only to FXO interfaces.
Out-of-Service (Busy Out) Parameters	
Web/EMS: Enable Busy Out **[EnableBusyOut]**	Determines whether the Busy Out feature is enabled. ▪ **[0]** Disable = 'Busy out' feature is not used (default). ▪ **[1]** Enable = 'Busy out' feature is enabled. When Busy Out is enabled and certain scenarios exist, the device performs the following: A reorder tone (configured by the parameter FXSOOSBehavior) is played when the phone is off-hooked. These behaviors are performed upon one of the following scenarios: ▪ Physically disconnected from the network (i.e., Ethernet cable is disconnected). ▪ The Ethernet cable is connected, but the device can't communicate with any host. Note that LAN Watch-Dog must be activated (the parameter EnableLANWatchDog set to 1). ▪ 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. ▪ The IP Connectivity mechanism is enabled (using the parameter AltRoutingTel2IPEnable) and there is no connectivity to any destination IP address. **Notes:** ▪ The FXSOOSBehavior parameter determines the behavior of the FXS endpoints when a Busy Out or Graceful Lock occurs. ▪ FXO endpoints during Busy Out and Lock are inactive. ▪ See the LifeLineType parameter for complementary optional behavior.
Web: Out-Of-Service Behavior EMS:FXS OOS Behavior **[FXSOOSBehavior]**	Determines the behavior of undefined FXS endpoints and all FXS endpoints when a Busy Out condition exists. ▪ **[0]** None = Normal operation. No response is provided to undefined endpoints. A dial tone is played to FXS endpoints when a Busy Out condition exists. ▪ **[1]** Reorder Tone = The device plays a reorder tone to the connected phone/PBX (default). ▪ **[2]** Polarity Reversal = The device reverses the polarity of the endpoint marking it unusable (relevant, for example, for PBX DID lines). This option can't be configured on-the-fly. ▪ **[3]** Reorder Tone + Polarity Reversal = Same as 2 and 3 combined. This option can't be configured on-the-fly. ▪ **[4]** Current Disconnect = The device disconnects the current of the FXS endpoint. This option can't be configured on-the-fly. **Note:** This parameter is applicable only to FXS interfaces.

Parameter	Description
Retransmission Parameters	
Web: SIP T1 Retransmission Timer **[msec]** EMS: T1 RTX **[SipT1Rtx]**	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. **Note:** The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx. For example (assuming that SipT1Rtx = 500 and SipT2Rtx = 4000): ▪ The first retransmission is sent after 500 msec. ▪ The second retransmission is sent after 1000 (2*500) msec. ▪ The third retransmission is sent after 2000 (2*1000) msec. ▪ The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec.
Web: SIP T2 Retransmission Timer **[msec]** EMS: T2 RTX **[SipT2Rtx]**	The maximum interval (in msec) between retransmissions of SIP messages. The default is 4000. **Note:** The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.
Web: SIP Maximum RTX EMS: Max RTX **[SIPMaxRtx]**	Maximum number of UDP transmissions (first transmission plus retransmissions) of SIP messages. The range is 1 to 30. The default value is 7.
Web: Number of RTX Before Hot-Swap EMS: Proxy Hot Swap Rtx **[HotSwapRtx]**	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 value is 3. **Note:** This parameter is also used for alternative routing using the 'Tel to IP Routing'. If a domain name in the 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.

10.10 Coders and Profile Parameters

The profile parameters are described in the table below.

Table 10-30: Profile Parameters

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td colspan="2">Web: Coders Table/Coder Group Settings
EMS: Coders Group</td></tr>
<tr><td>[CodersGroup0]
[CodersGroup1]
[CodersGroup2]
[CodersGroup3]
[CodersGroup4]</td><td>This ini file table parameter defines the device's coders. Up to five groups of coders can be defined, where each group can consist of up to 10 coders. The first Coder Group is the default coder list and the default Coder Group. These Coder Groups can later be assigned to IP or Tel Profiles.
The format of this parameter is as follows:
[CodersGroup0]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime, CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
[\CodersGroup0]
Where,
▪ Index = Coder entry 0-9, i.e., up to 10 coders per group.
▪ Name = Coder name.
▪ Ptime = Packetization time (ptime) - how many coder payloads are combined into a single RTP packet.
▪ Rate = Packetization rate.
▪ PayloadType = Identifies the format of the RTP payload.
▪ Sce = Enables silence suppression:
✓ [0] Disabled (default)
✓ [1] Enabled
For example, below are defined two Coder Groups (0 and 1):
[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 2 = eg711Ulaw, 10, 0, 71, 0;
[\CodersGroup0]
[CodersGroup1]
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;
[\CodersGroup1]
The table below lists the supported coders:
<table>
<tr><th>Coder Name</th><th>Packetization Time (msec)</th><th>Rate (kbps)</th><th>Payload Type</th><th>Silence Suppression</th></tr>
<tr><td>G.711 A-law [g711Alaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 8</td><td>Disable [0]
Enable [1]</td></tr>
<tr><td>G.711 U-law [g711Ulaw64k]</td><td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td><td>Always 64</td><td>Always 0</td><td>Disable [0]
Enable [1]</td></tr>
</table>
</td></tr>
</table>

Parameter	Description

G.711A-law_VBD **[g711AlawVbd]**	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Dynamic (0-127)	N/A
G.711U-law_VBD **[g711UlawVbd]**	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Dynamic (0-127)	N/A
EG.711 A-law **[eg711Alaw]**	10 (default), 20, 30	Always 64	Dynamic (96-127)	N/A
EG.711 U-law **[eg711Ulaw]**	10 (default), 20, 30	Always 64	Dynamic (96-127)	N/A
G.722 **[g722]**	20 (default), 40, 60, 80, 100, 120	64 (default)	Always 9	N/A
G.723.1 **[g7231]**	30 (default), 60, 90	5.3 **[0]** (default), 6.3 **[1]**	Always 4	Disable **[0]** Enable **[1]**
G.726 **[g726]**	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	16 **[0]** (default), 24 **[1]**, 32 **[2]**, 40 **[3]**	Dynamic (0-127) Default is 23	Disable **[0]** Enable **[1]**
G.727 ADPCM	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	16, 24, 32, 40	Dynamic (0-127)	Disable **[0]** Enable **[1]**
G.729 **[g729]**	10, 20 (default), 30, 40, 50, 60, 80, 100	Always 8	Always 18	Disable **[0]** Enable **[1]** Enable w/o Adaptations **[2]**
T.38 **[t38fax]**	N/A	N/A	N/A	N/A

Notes:

- The coder name is case-sensitive.
- Each coder type can appear only once per Coder Group.
- Only the packetization time of the first coder in the defined 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 defined for a specific coder, the value defined by the parameter EnableSilenceCompression is used.
- If G.729 is selected and silence suppression is enabled (for this coder), the device includes the string 'annexb=no' in the SDP of the relevant SIP messages. If silence suppression is set to 'Enable w/o Adaptations', 'annexb=yes' is included. An exception is when the remote device is a Cisco gateway (IsCiscoSCEMode).
- The coder G.722 provides Packet Loss Concealment (PLC) capabilities, ensuring higher voice quality.
- A Coder Group can be assigned to an IP Profile (using the IPProfile parameter) and/or to a Tel Profile (using the TelProfile parameter).
- For an explanation on V.152 support (and implementation of T.38 and

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>VBD coders), see "V.152 Support" on page 253.
▪ For a description of using ini file table parameters, see "Configuring ini File Table Parameters" on page 194.</td></tr>
<tr><td colspan="2">Web: IP Profile Settings Table
EMS: Protocol Definition > IP Profile</td></tr>
<tr><td>[IPProfile]</td><td>This ini file 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 Tel-to-IP routing rules (Prefix parameter), IP-to-Tel routing rules (PSTNPrefix parameter), and IP Groups (IPGroup parameter).
The format of this parameter is as follows:
[IPProfile]
FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference, IpProfile_CodersGroupID, IpProfile_IsFaxUsed, IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor, IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE, IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort, IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP, IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP, IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber, IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume, IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID, IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode, IpProfile_SBCAllowedCodersGroupID, IpProfile_SBCAllowedCodersMode, IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior, IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversionMode, IpProfile_SBCHistoryInfoMode;
[\IPProfile]
For example:
IPProfile 1 = ITSP, 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0, 0, -1, 1, 0, 0, -1, 1, 4, -1, 1, 1, 0, 0, , , -1, 0, 0, -1, 0, 0, 0, 0, -1, 0, 8, 300, 400, -1, -1;
Notes:
▪ You can configure up to nine IP Profiles (i.e., indices 1 through 9).
▪ To use the settings of the corresponding "global" parameter, enter the value -1 (or in the Web interface, the option 'Not Configured').
▪ For a detailed description of each parameter, see its corresponding global parameter:

<table>
<tr><th>IPProfile Field</th><th>Web Name</th><th>Global Parameter</th></tr>
<tr><td>IpProfile_Index</td><td>Profile ID</td><td>-</td></tr>
<tr><td>IpProfile_ProfileName</td><td>Profile Name</td><td>-</td></tr>
<tr><td>IpProfile_IpPreference</td><td>Profile Preference</td><td>-</td></tr>
</table>
</td></tr>
</table>

Parameter	Description		
	IpProfile_CodersGroupID	Coder Group	CodersGroup
	IpProfile_IsFaxUsed	Fax Signaling Method	IsFaxUsed
	IpProfile_JitterBufMinDelay	Dynamic Jitter Buffer Minimum Delay	DJBufMinDelay
	IpProfile_JitterBufOptFactor	Dynamic Jitter Buffer Optimization Factor	DJBufOptFactor
	IpProfile_IPDiffServ	RTP IP DiffServ	PremiumServiceClassMediaDiffServ
	IpProfile_SigIPDiffServ	Signaling DiffServ	PremiumServiceClassControlDiffServ
	IpProfile_SCE	-	EnableSilenceCompression
	IpProfile_RTPRedundancyDepth	RTP Redundancy Depth	RTPRedundancyDepth
	IpProfile_RemoteBaseUDPPort	Remote RTP Base UDP Port	RemoteBaseUDPPort
	IpProfile_CNGmode	CNG Detector Mode	CNGDetectorMode
	IpProfile_VxxTransportType	Modems Transport Type	V21ModemTransportType; V22ModemTransportType; V23ModemTransportType; V32ModemTransportType; V34ModemTransportType
	IpProfile_NSEMode	NSE Mode	NSEMode
	IpProfile_PlayRBTone2IP	Play Ringback Tone to IP	PlayRBTone2IP
	IpProfile_EnableEarlyMedia	Enable Early Media	EnableEarlyMedia
	IpProfile_ProgressIndicator2IP	Progress Indicator to IP	ProgressIndicator2IP
	IpProfile_EnableEchoCanceller	Echo Canceler	EnableEchoCanceller
	IpProfile_CopyDest2RedirectNumber	Copy Destination Number to Redirect Number	CopyDest2RedirectNumber
	IpProfile_MediaSecurityBehaviour	Media Security Behavior	MediaSecurityBehaviour
	IpProfile_CallLimit	Number of Calls Limit	-

Parameter	Description		
	IpProfile_DisconnectOnBrokenConnection	Disconnect on Broken Connection	DisconnectOnBroken Connection
	IpProfile_FirstTxDtmfOption	First Tx DTMF Option	TxDTMFOption
	IpProfile_SecondTxDtmfOption	Second Tx DTMF Option	TxDTMFOption
	IpProfile_RxDTMFOption	Declare RFC 2833 in SDP	RxDTMFOption
	IpProfile_EnableHold	Enable Hold	EnableHold
	IpProfile_InputGain	Input Gain	InputGain
	IpProfile_VoiceVolume	Voice Volume	VoiceVolume
	IpProfile_AddIEInSetup	Add IE In SETUP	AddIEinSetup
	IpProfile_SBCExtensionCodersGroupID	Extension Coders Group ID	SBCExtensionCoders GroupID
	IpProfile_MediaIPVersionPreference	Media IP Version Preference	MediaIPVersionPreference
	IpProfile_TranscodingMode	Transcoding Mode	TranscodingMode
	IpProfile_SBCAllowedCodersGroupID	Allowed Coders Mode	-
	IpProfile_SBCAllowedCodersMode	Allowed Coders Group ID	AllowedCodersGroup 0
	IpProfile_SBCMediaSecurityBehaviour	-	SBCMediaSecurityBehaviour
	IpProfile_SBCRFC2833Behavior	-	-
	IpProfile_SBCAlternativeDTMFMethod	-	-
	IpProfile_SBCAssertIdentity	-	SBCAssertIdentity
	IpProfile_AMDSensitivityParameterSuit	AMD Sensitivity Level	AMDSensitivityLevel
	IpProfile_AMDSensitivityLevel	AMD Sensitivity Level	AMDSensitivityLevel
	IpProfile_AMDMaxGreetingTime	AMD Max Greeting Time	AMDMaxGreetingTime
	IpProfile_AMDMaxPostSilenceGreetingTime	AMD Max Post Silence Greeting Time	AMDMaxPostGreetingSilenceTime

Parameter	Description
	IpProfile_SBCDiversionMode — Diversion Mode — -
	IpProfile_SBCHistoryInfoMode — History Info Mode — -
	▪ The parameter IpPreference determines the priority of the IP Profile (1 to 20, where 20 is the highest preference). If both IP and Tel Profiles apply to the same call, the coders and common parameters (i.e., parameters configurable in both IP and Tel Profiles) of the preferred profile are applied to that call. If the Tel and IP Profiles are identical, the Tel Profile parameters take precedence. ▪ The parameter CallLimit defines the maximum number of concurrent calls allowed for that Profile. If the Profile is set to some limit, the device maintains the number of concurrent calls (incoming and outgoing) pertaining to the specific Profile. A limit value of **[-1**] indicates that there is no limitation on calls (default). A limit value of **[0]** indicates that all calls are rejected. When the number of concurrent calls is equal to the limit, the device rejects any new incoming and outgoing calls pertaining to that profile. ▪ 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. ▪ FirstTxDtmfOption and SecondTxDtmfOption configures the transmit DTMF negotiation method: **[-1**] not configured, use the global parameter; for the remaining options, see the global parameter. ▪ The VxxTransportType parameter configures the modem transport type per IP Profile for the following parameters: V21ModemTransportType, V22ModemTransportType, V23ModemTransportType, V32ModemTransportType, and V34ModemTransportType. ▪ IP Profiles can also be used when operating with a Proxy server (set the parameter AlwaysUseRouteTable to 1). ▪ The following parameters are not applicable: IsDTMFUsed (deprecated), SBCExtensionCodersGroupID, TranscodingMode SBCAllowedCodersGroupID, SBCAllowedCodersMode, SBCMediaSecurityBehaviour, SBCRFC2833Behavior, SBCAlternativeDTMFMethod, SBCAssertIdentity, SBCDiversionMode, SBCHistoryInfoMode, AddIEInSetup MediaIPVersionPreference ▪ For a description of using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
Web: Tel Profile Settings Table **EMS: Protocol Definition > Telephony Profile**	
[TelProfile]	This *ini* file 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 Endpoint 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. The format of this parameter is as follows: [TelProfile] FORMAT TelProfile_Index = TelProfile_ProfileName, TelProfile_TelPreference, TelProfile_CodersGroupID, TelProfile_IsFaxUsed,

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>
TelProfile_JitterBufMinDelay, TelProfile_JitterBufOptFactor, TelProfile_IPDiffServ, TelProfile_SigIPDiffServ, TelProfile_DtmfVolume, TelProfile_InputGain, TelProfile_VoiceVolume, TelProfile_EnableReversePolarity, TelProfile_EnableCurrentDisconnect, TelProfile_EnableDigitDelivery, TelProfile_EnableEC, TelProfile_MWIAnalog, 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_ECNlpMode;
TelProfile_DigitalCutThrough;
[\TelProfile]
For example:
TelProfile 1 = ITSP_audio, 1, 0, 0, 10, 10, 46, 40, -11, 0, 0, 0, 0, 0, 1, 0, 0, 700, 0, -1, 255, 0, 1, 1, 1, -1, 1, 0, 0, 0, 0;
Notes:

You can configure up to nine Tel Profiles (i.e., indices 1 through 9).
To use the settings of the corresponding global parameter, enter the value -1 (or in the Web interface, the option 'Not Configured').
For a detailed description of each parameter, see its corresponding "global" parameter:

<table>
<tr><th>TelProfile Field</th><th>Web Name</th><th>Global Parameter</th></tr>
<tr><td>TelProfile_ProfileName</td><td>Profile Name</td><td>-</td></tr>
<tr><td>TelProfile_TelPreference</td><td>Profile Preference</td><td>-</td></tr>
<tr><td>TelProfile_CodersGroupID</td><td>Coder Group</td><td>CodersGroup0</td></tr>
<tr><td>TelProfile_IsFaxUsed</td><td>Fax Signaling Method</td><td>IsFaxUsed</td></tr>
<tr><td>TelProfile_JitterBufMinDelay</td><td>Dynamic Jitter Buffer Minimum Delay</td><td>DJBufMinDelay</td></tr>
<tr><td>TelProfile_JitterBufOptFactor</td><td>Dynamic Jitter Buffer Optimization Factor</td><td>DJBufOptFactor</td></tr>
<tr><td>TelProfile_IPDiffServ</td><td>RTP IP DiffServ</td><td>PremiumServiceClassMediaDiffServ</td></tr>
<tr><td>TelProfile_SigIPDiffServ</td><td>Signaling DiffServ</td><td>PremiumServiceClassControlDiffServ</td></tr>
<tr><td>TelProfile_DtmfVolume</td><td>DTMF Volume</td><td>DTMFVolume</td></tr>
<tr><td>TelProfile_InputGain</td><td>Input Gain</td><td>InputGain</td></tr>
<tr><td>TelProfile_VoiceVolume</td><td>Voice Volume</td><td>VoiceVolume</td></tr>
<tr><td>TelProfile_EnableReversePolarity</td><td>Enable Polarity Reversal</td><td>EnableReversalPolarity</td></tr>
</table>
</td></tr>
</table>

Parameter	Description
	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 — SwapTEl2IPCalled&CallingNumbers **TelProfile_EnableAGC** — Enable AGC — EnableAGC **TelProfile_ECNlpMode** — EC NLP Mode — ECNLPMode **TelProfile_DigitalCutThrough** — - — DigitalCutThrough ▪ The parameter IpPreference determines the priority of the Tel Profile (1 to 20, where 20 is the highest preference). If both IP and Tel Profiles apply to the same call, the coders and common parameters (i.e., parameters configurable in both IP and Tel Profiles) of the preferred profile are applied to that call. If the Tel and IP Profiles are identical, the Tel Profile

Parameter	Description
	parameters take precedence. ▪ The parameter EnableVoiceMailDelay is applicable only if voice mail is enabled globally (using the VoiceMailInterface parameter). ▪ For a description of using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.11 Channel Parameters

This subsection describes the device's channel parameters.

10.11.1 Voice Parameters

The voice parameters are described in the table below.

Table 10-31: Voice Parameters

Parameter	Description
Web/EMS: Input Gain **[InputGain]**	Pulse-code modulation (PCM) input gain control (in decibels). This parameter sets the level for the received (Tel-to-IP) signal. The valid range is -32 to 31 dB. The default value is 0 dB. **Note:** This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122) and per Tel Profile, using the TelProfile parameter (see "Configuring Tel Profiles" on page 121).
Web: Voice Volume EMS: Volume (dB) **[VoiceVolume]**	Voice gain control (in decibels). This parameter sets the level for the transmitted (IP-to-Tel) signal. The valid range is -32 to 31 dB. The default value is 0 dB. **Note:** This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122) and per Tel Profile, using the TelProfile parameter (see "Configuring Tel Profiles" on page 121).
EMS: Payload Format **[VoicePayloadFormat]**	Determines the bit ordering of the G.726/G.727 voice payload format. ▪ **[0]** = Little Endian (default) ▪ **[1]** = Big Endian **Note:** 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 **[MFTransportType]**	Currently, not supported.
Web: Enable Answer Detector **[EnableAnswerDetector]**	Currently, not supported.
Web: Answer Detector Activity Delay **[AnswerDetectorActivityDelay]**	Determines (in 100-msec resolution) the time between activating the Answer Detector and the time that the detector actually starts to operate. The valid range is 0 to 1023. The default is 0.

Parameter	Description
Web: Answer Detector Silence Time **[AnswerDetectorSilenceTime]**	Currently, not supported.
Web: Answer Detector Redirection **[AnswerDetectorRedirection]**	Currently, not supported.
Web: Answer Detector Sensitivity EMS: Sensitivity **[AnswerDetectorSensitivity]**	Determines 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 **[EnableSilenceCompression]**	Silence Suppression is a method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. ▪ **[0]** Disable = Silence Suppression is disabled (default). ▪ **[1]** Enable = Silence Suppression is enabled. ▪ **[2]** Enable without Adaptation = A single silence packet is sent during a silence period (applicable only to G.729). **Note:** If the selected coder is G.729, the value of the 'annexb' parameter of the fmtp attribute in the SDP is determined by the following rules: ▪ If EnableSilenceCompression is 0: 'annexb=no'. ▪ If EnableSilenceCompression is 1: 'annexb=yes'. ▪ If EnableSilenceCompression is 2 and IsCiscoSCEMode is 0: 'annexb=yes'. ▪ If EnableSilenceCompression is 2 and IsCiscoSCEMode is 1: 'annexb=no'. **Note:** This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Web: Echo Canceler EMS: Echo Canceller Enable **[EnableEchoCanceller]**	Enables or disables echo cancellation (i.e., echo from voice calls is removed). ▪ **[0]** Off = Echo Canceler is disabled. ▪ **[1]** On = Echo Canceler is enabled (default). **Notes:** ▪ This parameter is used to maintain backward compatibility. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122) and per Tel Profile, using the TelProfile parameter (see "Configuring Tel Profiles" on page 121).
EMS: Echo Canceller Hybrid Loss **[ECHybridLoss]**	Sets 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. ▪ **[0]** = 6 dB (default) ▪ **[1]** = N/A ▪ **[2]** = 0 dB ▪ **[3]** = 3 dB

Parameter	Description
[ECNLPMode]	Defines the echo cancellation Non-Linear Processing (NLP) mode. ▪ **[0]** = NLP adapts according to echo changes (default). ▪ **[1]** = Disables NLP. ▪ **[2]** = Silence output NLP. **Note:** This parameter can also be configured per Tel Profile, using the TelProfile parameter (see "Configuring Tel Profiles" on page 121).
[EchoCancellerAggressiveNLP]	Enables or disables the Aggressive NLP at the first 0.5 second of the call. When enabled, the echo is removed only in the first half of a second of the incoming IP signal. ▪ **[0]** = Disable ▪ **[1]** = Enable (default) **Note:** For this parameter to take effect, a device reset is required.
[RTPSIDCoeffNum]	Determines the number of spectral coefficients added to an SID packet being sent according to RFC 3389. The valid values are **[0]** (default), **[4]**, **[6]**, **[8]** and **[10]**.

10.11.2 Coder Parameters

The coder parameters are described in the table below.

Table 10-32: Coder Parameters

Parameter	Description
Web: DSP Version Template Number EMS: Version Template Number **[DSPVersionTemplateNumber]**	Determines the DSP template to use on the device. Each DSP template supports specific coders, channel capacity, and features. For the list of supported DSP templates, refer to the Release Notes. The default is DSP template 0.

10.11.3 Fax and Modem Parameters

The fax and modem parameters are described in the table below.

Table 10-33: Fax and Modem Parameters

Parameter	Description
Web: Fax Transport Mode EMS: Transport Mode **[FaxTransportMode]**	Fax transport mode used by the device. ▪ **[0]** Disable = transparent mode ▪ **[1]** T.38 Relay (default) ▪ **[2]** Bypass ▪ **[3]** Events Only **Note:** 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).

Parameter	Description
Web: Fax Relay Enhanced Redundancy Depth EMS: Enhanced Relay Redundancy Depth **[FaxRelayEnhancedRedundancyDepth]**	Number of times that control packets are retransmitted when using the T.38 standard. The valid range is 0 to 4. The default value is 2.
Web: Fax Relay Redundancy Depth EMS: Relay Redundancy Depth **[FaxRelayRedundancyDepth]**	Number of times that each fax relay payload is retransmitted to the network. ▪ **[0]** = No redundancy (default). ▪ **[1]** = One packet redundancy. ▪ **[2]** = Two packet redundancy. **Note:** This parameter is applicable only to non-V.21 packets.
Web: Fax Relay Max Rate (bps) EMS: Relay Max Rate **[FaxRelayMaxRate]**	Maximum rate (in bps) at which fax relay messages are transmitted (outgoing calls). ▪ **[0]** 2400 = 2.4 kbps ▪ **[1]** 4800 = 4.8 kbps ▪ **[2]** 7200 = 7.2 kbps ▪ **[3]** 9600 = 9.6 kbps ▪ **[4]** 12000 = 12.0 kbps ▪ **[5]** 14400 = 14.4 kbps (default) ▪ **[6]** 16800bps = 16.8 kbps ▪ **[7]** 19200bps = 19.2 kbps ▪ **[8]** 21600bps = 21.6 kbps ▪ **[9]** 24000bps = 24 kbps ▪ **[10]** 26400bps = 26.4 kbps ▪ **[11]** 28800bps = 28.8 kbps ▪ **[12]** 31200bps = 31.2 kbps ▪ **[13]** 33600bps = 33.6 kbps **Notes:** ▪ 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. ▪ Configuration above 14.4 kbps is truncated to 14.4 kbps for non-T.38 V.34 supporting devices.
Web: Fax Relay ECM Enable EMS: Relay ECM Enable **[FaxRelayECMEnable]**	Determines whether the Error Correction Mode (ECM) mode is used during fax relay. ▪ **[0]** Disable = ECM mode is not used during fax relay. ▪ **[1]** Enable = ECM mode is used during fax relay (default).
Web: Fax/Modem Bypass Coder Type EMS: Coder Type **[FaxModemBypassCoderType]**	Coder used by the device when performing fax/modem bypass. Usually, high-bit-rate coders such as G.711 should be used. ▪ **[0]** G.711Alaw= G.711 A-law 64 (default). ▪ **[1]** G.711Mulaw = G.711 μ-law.

Parameter	Description
Web/EMS: CNG Detector Mode **[CNGDetectorMode]**	Determines whether the device detects the fax Calling tone (CNG). ▪ **[0]** Disable = The originating device doesn't detect CNG; the CNG signal passes transparently to the remote side (default). ▪ **[1]** 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. ▪ **[2]** 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. **Note:** This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Web: Fax/Modem Bypass Packing Factor EMS: Packetization Period **[FaxModemBypassM]**	Number of (20 msec) coder payloads that are used to generate a fax/modem bypass packet. The valid range is 1, 2, or 3 coder payloads. The default value is 1 coder payload.
[FaxModemNTEMode]	Determines whether the device sends RFC 2833 ANS/ANSam events upon detection of fax and/or modem Answer tones (i.e., CED tone). ▪ **[0]** = Disabled (default). ▪ **[1]** = Enabled. **Note:** This parameter is applicable only when the fax or modem transport type is set to bypass or Transparent-with-Events.
Web/EMS: Fax Bypass Payload Type **[FaxBypassPayloadType]**	Determines the fax bypass RTP dynamic payload type. The valid range is 96 to 120. The default value is 102.
EMS: Modem Bypass Payload Type **[ModemBypassPayloadType]**	Modem Bypass dynamic payload type. The range is 0-127. The default value is 103.
EMS: Relay Volume (dBm) **[FaxModemRelayVolume]**	Determines 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 **[FaxBypassOutputGain]**	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).

Parameter	Description
Web/EMS: Modem Bypass Output Gain **[ModemBypassOutputGain]**	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: NTE Max Duration **[NTEMaxDuration]**	Maximum time for sending Named Telephony Events (NTEs) to the IP side regardless of the time range when the TDM signal is detected. The range is -1 to 200,000,000 msec (i.e., 55 hours). The default is -1 (i.e., NTE stops only upon detection of an End event).
EMS: Basic Packet Interval **[FaxModemBypassBasicRTPPacketInterval]**	Determines the basic frame size that is used during fax/modem bypass sessions. ▪ **[0]** = Determined internally (default) ▪ **[1]** = 5 msec (not recommended) ▪ **[2]** = 10 msec ▪ **[3]** = 20 msec **Note:** When set to 5 msec (1), the maximum number of simultaneous channels supported is 120.
EMS: Dynamic Jitter Buffer Minimal Delay (dB) **[FaxModemBypasDJBufMinDelay]**	Determines 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 **[EnableFaxModemInbandNetworkDetection]**	Enables or disables in-band network detection related to fax/modem. ▪ **[0]** = Disable (default) ▪ **[1]** = 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.
EMS: NSE Mode **[NSEMode]**	Cisco compatible fax and modem bypass mode. ▪ **[0]** = NSE disabled (default) ▪ **[1]** = NSE enabled In NSE bypass mode, the device starts using G.711 A-Law (default) or G.711μ-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 μ-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. **Notes:** ▪ This feature can be used only if the VxxModemTransportType parameter is set to 2 (Bypass). ▪ If NSE mode is enabled, the SDP contains the following line:

Parameter	Description
	'a=rtpmap:100 X-NSE/8000'. ▪ To use this feature: ✓ The Cisco gateway must include the following definition: 'modem passthrough nse payload-type 100 codec g711alaw'. ✓ Set the Modem transport type to Bypass mode (VxxModemTransportType is set to 2) for all modems. ✓ Configure the gateway parameter NSEPayloadType = 100. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
EMS: NSE Payload Type **[NSEPayloadType]**	NSE payload type for Cisco Bypass compatible mode. The valid range is 96-127. The default value is 105. **Note:** Cisco gateways usually use NSE payload type of 100.
Web: V.21 Modem Transport Type EMS: V21 Transport **[V21ModemTransportType]**	V.21 Modem Transport Type used by the device. ▪ **[0]** Disable = Disable (Transparent) - default ▪ **[1]** Enable Relay = N/A ▪ **[2]** Enable Bypass. ▪ **[3]** Events Only = Transparent with Events **Note:** This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Web: V.22 Modem Transport Type EMS: V22 Transport **[V22ModemTransportType]**	V.22 Modem Transport Type used by the device. ▪ **[0]** Disable = Disable (Transparent) ▪ **[1]** Enable Relay = N/A ▪ **[2]** Enable Bypass = (default) ▪ **[3]** Events Only = Transparent with Events **Note:** This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Web: V.23 Modem Transport Type EMS: V23 Transport **[V23ModemTransportType]**	V.23 Modem Transport Type used by the device. ▪ **[0]** Disable = Disable (Transparent) ▪ **[1]** Enable Relay = N/A ▪ **[2]** Enable Bypass = (default) ▪ **[3]** Events Only = Transparent with Events **Note:** This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Web: V.32 Modem Transport Type EMS: V32 Transport **[V32ModemTransportType]**	V.32 Modem Transport Type used by the device. ▪ **[0]** Disable = Disable (Transparent) ▪ **[1]** Enable Relay = N/A ▪ **[2]** Enable Bypass = (default) ▪ **[3]** Events Only = Transparent with Events **Notes:** ▪ This parameter applies only to V.32 and V.32bis modems. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).

Parameter	Description
Web: V.34 Modem Transport Type EMS: V34 Transport **[V34ModemTransportType]**	V.90/V.34 Modem Transport Type used by the device. ▪ **[0]** Disable = Disable (Transparent) ▪ **[1]** Enable Relay = N/A ▪ **[2]** Enable Bypass = (default) ▪ **[3]** Events Only = Transparent with Events **Note:** This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
EMS: Bell Transport Type **[BellModemTransportType]**	Determines the Bell modem transport method. ▪ **[0]** = Transparent (default) ▪ **[2]** = Bypass ▪ **[3]** = Transparent with events

10.11.4 DTMF Parameters

The dual-tone multi-frequency (DTMF) parameters are described in the table below.

Table 10-34: DTMF Parameters

Parameter	Description
Web/EMS: DTMF Transport Type **[DTMFTransportType]**	Determines the DTMF transport type. ▪ **[0]** DTMF Mute = Erases digits from voice stream and doesn't relay to remote. ▪ **[2]** Transparent DTMF = Digits remain in voice stream. ▪ **[3]** RFC 2833 Relay DTMF = Erases digits from voice stream and relays to remote according to RFC 2833 (default). ▪ **[7]** RFC 2833 Relay Rcv Mute = DTMFs are sent according to RFC 2833 and muted when received. **Note:** This parameter is automatically updated if the parameters TxDTMFOption or RxDTMFOption are configured.
Web: DTMF Volume (-31 to 0 dB) EMS: DTMF Volume (dBm) **[DTMFVolume]**	DTMF gain control value (in decibels) to the or analog side. The valid range is -31 to 0 dB. The default value is -11 dB. **Note:** This parameter can also be configured per Tel Profile, using the TelProfile parameter.
Web: DTMF Generation Twist EMS: DTMF Twist Control **[DTMFGenerationTwist]**	Defines the range (in decibels) between the high and low frequency components in the DTMF signal. Positive decibel values cause the higher frequency component to be stronger than the lower one. Negative values cause the opposite effect. For any parameter value, both components change so that their average is constant. The valid range is -10 to 10 dB. The default value is 0 dB. **Note:** For this parameter to take effect, a device reset is required.
EMS: DTMF Inter Interval (msec) **[DTMFInterDigitInterval]**	Time in msec between generated DTMF digits to PSTN side (if TxDTMFOption = 1, 2 or 3). The default value is 100 msec. The valid range is 0 to 32767.

Parameter	Description
EMS: DTMF Length (msec) **[DTMFDigitLength]**	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. The valid range is 0 to 32767. The default value is 100.
EMS: Rx DTMF Relay Hang Over Time (msec) **[RxDTMFHangOverTime]**	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. Valid range is 0 to 2,000 msec. The default is 1,000 msec.
EMS: Tx DTMF Relay Hang Over Time (msec) **[TxDTMFHangOverTime]**	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. Valid range is 0 to 2,000 msec. The default is 1,000 msec.

10.11.5 RTP, RTCP and T.38 Parameters

The RTP, RTCP and T.38 parameters are described in the table below.

Table 10-35: RTP/RTCP and T.38 Parameters

Parameter	Description
Web: Dynamic Jitter Buffer Minimum Delay EMS: Minimal Delay (dB) **[DJBufMinDelay]**	Minimum delay (in msec) for the Dynamic Jitter Buffer. The valid range is 0 to 150. The default delay is 10. **Notes:** ▪ This parameter can also be configured per IP Profile or Tel Profile, using the IPProfile and TelProfile parameters respectively. ▪ For more information on Jitter Buffer, see "Dynamic Jitter Buffer Operation" on page 227.
Web: Dynamic Jitter Buffer Optimization Factor EMS: Opt Factor **[DJBufOptFactor]**	Dynamic Jitter Buffer frame error/delay optimization factor. The valid range is 0 to 12. The default factor is 10. **Notes:** ▪ For data (fax and modem) calls, set this parameter to 12. ▪ This parameter can also be configured per IP Profile or Tel Profile, using the IPProfile and TelProfile parameters respectively. ▪ For more information on Jitter Buffer, see "Dynamic Jitter Buffer Operation" on page 227.
Web/EMS: Analog Signal Transport Type **[AnalogSignalTransportType]**	Determines the analog signal transport type. ▪ **[0]** Ignore Analog Signals = Ignore (default). ▪ **[1]** RFC 2833 Analog Signal Relay = Transfer hookflash using RFC 2833.
Web: RTP Redundancy Depth EMS: Redundancy Depth **[RTPRedundancyDepth]**	Determines whether the device generates redundant packets. This can be used for packet loss where the missing information (audio) can be reconstructed at the receiver end from the redundant data that arrives in the subsequent packet(s). ▪ **[0]** 0 = Disable the generation of redundant packets (default). ▪ **[1]** 1 = Enable the generation of RFC 2198 redundancy packets (payload type defined by the parameter

Parameter	Description
	RFC2198PayloadType). **Notes:** ▪ The RTP redundancy dynamic payload type can be included in the SDP, by using the parameter EnableRTPRedundancyNegotiation. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter.
Web: Enable RTP Redundancy Negotiation **[EnableRTPRedundancyNegotiation]**	Determines whether the device includes the RTP redundancy dynamic payload type in the SDP, according to RFC 2198. ▪ **[0]** Disable (default) ▪ **[1]** Enable When enabled, the device includes in the SDP message the RTP payload type "RED" and the payload type configured by the parameter RFC2198PayloadType. `a=rtpmap:<PT> RED/8000` Where *<PT>* is the payload type as defined by RFC2198PayloadType. The device sends the INVITE message with "a=rtpmap:<PT> RED/8000" and responds with a 18x/200 OK and "a=rtpmap:<PT> RED/8000" in the SDP. **Notes:** ▪ For this feature to be functional, you must also set the parameter RTPRedundancyDepth to 1 (i.e., enabled). ▪ Currently, the negotiation of “RED” payload type is not supported and therefore, it should be configured to the same PT value for both parties.
Web: RFC 2198 Payload Type EMS: Redundancy Payload Type **[RFC2198PayloadType]**	RTP redundancy packet payload type according to RFC 2198. The range is 96 to 127. The default is 104. **Note:** This parameter is applicable only if the parameter RTPRedundancyDepth is set to 1.
Web: Packing Factor EMS: Packetization Factor **[RTPPackingFactor]**	N/A. Controlled internally by the device according to the selected coder.
Web/EMS: Basic RTP Packet Interval **[BasicRTPPacketInterval]**	N/A. Controlled internally by the device according to the selected coder.
Web: RTP Directional Control **[RTPDirectionControl]**	N/A. Controlled internally by the device according to the selected coder.
Web/EMS: RFC 2833 TX Payload Type **[RFC2833TxPayloadType]**	N/A. Use the *ini* file parameter RFC2833PayloadType instead.
Web/EMS: RFC 2833 RX Payload Type **[RFC2833RxPayloadType]**	N/A. Use the *ini* file parameter RFC2833PayloadType instead.

Parameter	Description
[EnableDetectRemoteMACChange]	Changes the RTP packets according to the MAC address of received RTP packets and according to Gratuitous Address Resolution Protocol (GARP) messages. ▪ **[0]** = Nothing is changed. ▪ **[1]** = If the device receives RTP packets with a different source MAC address (than the MAC address of the transmitted RTP packets), then it sends RTP packets to this MAC address and removes this IP entry from the device's ARP cache table. ▪ **[2]** = The device uses the received GARP packets to change the MAC address of the transmitted RTP packets (default). ▪ **[3]** = Options 1 and 2 are used. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ If the device is located in a network subnet which is connected to other gateways using a router that uses Virtual Router Redundancy Protocol (VRRP) for redundancy, then set this parameter to 0 or 2.
Web: RTP Base UDP Port EMS: Base UDP Port **[BaseUDPport]**	Lower boundary of the UDP port used for RTP, RTCP (RTP port + 1) and T.38 (RTP port + 2). The upper boundary of the UDP port range is the Base UDP Port + 10 * number of the device's channels. The range of possible UDP ports is 6,000 to 64,000. The default base UDP port is 6000. For example, if the Base UDP Port is set to 6000, then 1) one channel may use the ports RTP 6000, RTCP 6001, and T.38 6002, 2) another channel may use RTP 6010, RTCP 6011, and T.38 6012, etc. The UDP port range is as follows: ▪ MP-112/MP-114: BaseUDPport to BaseUDPport + 3*10 ▪ MP-118: BaseUDPport to BaseUDPport + 7*10 ▪ MP-124: BaseUDPport to BaseUDPport + 23*10 **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ The UDP ports are allocated randomly to channels. ▪ You can define a UDP port range per Media Realm (see Configuring Media Realms). ▪ If RTP Base UDP Port is not a factor of 10, the following message is generated: 'invalid local RTP port'. ▪ For detailed information on the default RTP/RTCP/T.38 port allocation, refer to the *Product Reference Manual*.
Web: Remote RTP Base UDP Port EMS: Remote Base UDP Port **[RemoteBaseUDPPort]**	Determines the lower boundary of UDP ports used for RTP, RTCP and T.38 by a remote device. If this parameter is set to a non-zero value, ThroughPacket™ (RTP multiplexing) is enabled. The device uses this parameter (and BaseUDPPort) to identify and distribute the payloads from the received multiplexed IP packet to the relevant channels. The valid range is the range of possible UDP ports: 6,000 to 64,000.

Parameter	Description
	The default value is 0 (i.e., RTP multiplexing is disabled). For detailed information on RTP multiplexing, see RTP Multiplexing (ThroughPacket) on page 310. **Notes:** ▪ The value of this parameter on the local device must equal the value of BaseUDPPort on the remote device. ▪ When VLANs are implemented, RTP multiplexing is not supported. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter.
EMS: No Op Enable **[NoOpEnable]**	Enables or disables the transmission of RTP or T.38 No-Op packets. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable This mechanism ensures that the NAT binding remains open during RTP or T.38 silence periods.
EMS: No Op Interval **[NoOpInterval]**	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. The valid range is 20 to 65,000 msec. The default is 10,000. **Note:** To enable No-Op packet transmission, use the NoOpEnable parameter.
EMS: No Op Payload Type **[RTPNoOpPayloadType]**	Determines the payload type of No-Op packets. 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 value is 120. **Note:** When defining this parameter, ensure that it doesn't cause collision with other payload types.
Web: RTCP Packet Interval EMS: Packet Interval **[RTCPInterval]**	Defines the time interval (in msec) between adjacent RTCP reports. The interval range is 0 to 65,535. The default interval is 5,000.
Web: Disable RTCP Interval Randomization EMS: Disable Interval Randomization **[DisableRTCPRandomize]**	Controls whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter RTCPInterval. ▪ **[0]** Disable = Randomize (default) ▪ **[1]** Enable = No Randomize

10.12 Gateway and IP-to-IP Parameters

10.12.1 Fax and Modem Parameters

The fax and modem parameters are described in the table below.

Table 10-36: Fax and Modem Parameters

Parameter	Description
EMS: T38 Use RTP Port **[T38UseRTPPort]**	Defines the port (with relation to RTP port) for sending and receiving T.38 packets. ▪ **[0]** = Use the RTP port +2 to send/receive T.38 packets (default). ▪ **[1]** = Use the same port as the RTP port to send/receive T.38 packets. **Notes:** ▪ For this parameter to take effect, you must reset the device. ▪ 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 parameter T38UseRTPPort to 0.
Web/EMS: T.38 Max Datagram Size **[T38MaxDatagramSize]**	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. The valid range is 120 to 600. The default value is 238.
Web/EMS: T38 Fax Max Buffer **[T38FaxMaxBufferSize]**	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. The valid range is 500 to 3000. The default value is 1024.
Web/EMS: Enable Fax Re-Routing **[EnableFaxReRouting]**	Enables or disables re-routing of Tel-to-IP calls that are identified as fax calls. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = Enabled. If a CNG tone is detected on the Tel side of a Tel-to-IP call, the prefix "FAX" is appended to the destination number before routing and manipulations. A value of "FAX" entered as the destination number in the 'Tel to IP Routing' is then used to route the call and the destination number manipulation mechanism is used to remove the "FAX" prefix, if required. 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 tear down the voice call. **Notes:** ▪ To enable this feature, set the parameter CNGDetectorMode to 2 and the parameter IsFaxUsed to 1, 2, or 3. ▪ The "FAX" prefix in routing and manipulation tables is case-sensitive.

Parameter	Description
Web/EMS: Fax CNG Mode **[FaxCNGMode]**	Determines the device's behavior upon detection of a CNG tone. ▪ **[0]** = Does not send a SIP Re-INVITE upon detection of a fax CNG tone when the parameter CNGDetectorMode is set to 1 (default). ▪ **[1]** = Sends a SIP Re-INVITE upon detection of a fax CNG tone when the parameter CNGDetectorMode is set to 1.
Web: Detect Fax on Answer Tone EMS: Enables Detection of FAX on Answer Tone **[DetFaxOnAnswerTone]**	Determines when the device initiates a T.38 session for fax transmission. ▪ **[0]** Initiate T.38 on Preamble = The device to which the called fax is connected initiates a T.38 session on receiving HDLC Preamble signal from the fax (default). ▪ **[1]** 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. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ This parameters is applicable only if the parameter IsFaxUsed is set to 1 (T.38 Relay) or 3 (Fax Fallback).
[T38FaxSessionImmediateStart]	Enables fax transmission of T.38 “no-signal” packets to the terminating fax machine. ▪ **[0]** Disable (default) ▪ **[1]** Enable This is used for transmission from fax machines (connected to the device) located inside a Network Address Translation (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. 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. **Note:** To enable No-Op packet transmission, use the NoOpEnable and NoOpInterval parameters.

10.12.2 DTMF and Hook-Flash Parameters

The DTMF and hook-flash parameters are described in the table below.

Table 10-37: DTMF and Hook-Flash Parameters

Parameter	Description
Hook-Flash Parameters	
Web/EMS: Hook-Flash Code **[HookFlashCode]**	Defines the digit pattern that when received from the Tel side, indicates a Hook Flash event. The valid range is a 25-character string. The default is a null string. **Note:** This parameter can also be configured per Tel Profile, using the TelProfile parameter.
Web/EMS: Hook-Flash Option **[HookFlashOption]**	Determines the hook-flash transport type (i.e., method by which hook-flash is sent and received). ▪ **[0]** Not Supported = Hook-Flash indication isn't sent (default). ▪ **[1]** INFO = Sends proprietary INFO message with Hook-Flash indication. ▪ **[4]** RFC 2833 ▪ **[5]** INFO (Lucent) = Sends proprietary SIP INFO message with Hook-Flash indication. ▪ **[6]** INFO (NetCentrex) = 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 ▪ **[7]** INFO (HUAWAEI) = 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 **Notes:** ▪ FXO interfaces support only the receipt of RFC 2833 Hook-Flash signals and INFO **[1]** type. ▪ FXS interfaces send Hook-Flash signals only if the parameter EnableHold is set to 0.
Web: Min. Flash-Hook Detection Period **[msec]** EMS: Min Flash Hook Time **[MinFlashHookTime]**	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. The valid range is 25 to 300. The default value is 300. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is applicable only to FXS interfaces. ▪ 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).

Parameter	Description
Web: Max. Flash-Hook Detection Period **[msec]** EMS: Flash Hook Period **[FlashHookPeriod]**	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. For the analog side, it defines the following: ▪ FXS interfaces: ✓ Maximum hook-flash detection period. A longer signal is considered an off-hook or on-hook event. ✓ Hook-flash generation period upon detection of a SIP INFO message containing a hook-flash signal. ▪ FXO interfaces: Hook-flash generation period. The valid range is 25 to 3,000. The default value is 700. **Notes:** ▪ For this parameter to take effect, you need to reset the device. ▪ For FXO interfaces, a constant of 100 msec must be added to the required hook-flash period. For example, to generate a 450 msec hook-flash, set this parameter to 550. ▪ This parameter can also be configured per Tel Profile, using the TelProfile parameter.
DTMF Parameters	
EMS: Use End of DTMF **[MGCPDTMFDetectionPoint]**	Defines when the detection of DTMF events is notified. ▪ **[0]** = DTMF event is reported at the end of a detected DTMF digit. ▪ **[1]** = DTMF event is reported at the start of a detected DTMF digit (default).
Web: Declare RFC 2833 in SDP EMS: Rx DTMF Option **[RxDTMFOption]**	Defines the supported receive DTMF negotiation method. ▪ **[0]** No = Don't declare RFC 2833 telephony-event parameter in SDP. ▪ **[3]** Yes = Declare RFC 2833 telephony-event parameter in SDP (default). 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. **Note:** This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).

Parameter	Description
Web/EMS: Tx DTMF Option **[TxDTMFOption]**	Determines a single or several preferred transmit DTMF negotiation methods. ▪ **[0]** Not Supported = No negotiation - DTMF digits are sent according to the parameters DTMFTransportType and RFC2833PayloadType (default). ▪ **[1]** INFO (Nortel) = Sends DTMF digits according to IETF Internet-Draft draft-choudhuri-sip-info-digit-00. ▪ **[2]** NOTIFY = Sends DTMF digits according to IETF Internet-Draft draft-mahy-sipping-signaled-digits-01. ▪ **[3]** INFO (Cisco) = Sends DTMF digits according to Cisco format. ▪ **[4]** RFC 2833. ▪ **[5]** INFO (Korea) = Sends DTMF digits according to Korea Telecom format. **Notes:** ▪ DTMF negotiation methods are prioritized according to the order of their appearance. ▪ When out-of-band DTMF transfer is used (**[1], [2], [3],** or **[5]),** the parameter DTMFTransportType is automatically set to 0 (DTMF digits are erased from the RTP stream). ▪ When RFC 2833 (4) is selected, the device: **a.** Negotiates RFC 2833 payload type using local and remote SDPs. **b.** Sends DTMF packets using RFC 2833 payload type according to the payload type in the received SDP. **c.** Expects to receive RFC 2833 packets with the same payload type as configured by the parameter RFC2833PayloadType. **d.** Removes DTMF digits in transparent mode (as part of the voice stream). ▪ When TxDTMFOption is set to 0, the RFC 2833 payload type is set according to the parameter RFC2833PayloadType for both transmit and receive. ▪ The *ini* file table parameter TxDTMFOption can be repeated twice for configuring the DTMF transmit methods. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Web/EMS: Tx DTMF Option Table	
[TxDTMFOption]	This *ini* file table parameter configures up to two preferred transmit DTMF negotiation methods. The format of this parameter is as follows: [TxDTMFOption] FORMAT TxDTMFOption_Index = TxDTMFOption_Type; [\TxDTMFOption] For example: TxDTMFOption 0 = 1; TxDTMFOption 1 = 3; **Notes:**

Parameter	Description
	▪ This parameter can include up two indices. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122). ▪ For a description on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
[DisableAutoDTMFMute]	Enables/disables the automatic muting of DTMF digits when out-of-band DTMF transmission is used. ▪ **[0]** = Automatic mute is used (default). ▪ **[1]** = No automatic mute of in-band DTMF. 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. **Note:** Usually this mode is not recommended.
Web/EMS: Enable Digit Delivery to IP **[EnableDigitDelivery2IP]**	The Digit Delivery feature enables sending DTMF digits to the destination IP address after the Tel-to-IP call is answered. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = Enable digit delivery to IP. 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). **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ The called number can include several 'p' characters (1.5 seconds pause), for example, 1001pp699, 8888p9p300.
Web: Enable Digit Delivery to Tel EMS: Enable Digit Delivery **[EnableDigitDelivery]**	Enables the Digit Delivery feature, which sends DTMF digits of the called number to the device's port (phone line) after the call is answered (i.e., line is off-hooked for FXS, or seized for FXO) for IP-to-Tel calls. ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = Enable Digit Delivery feature for the FXO/FXS device. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ 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

Parameter	Description
	number can be as follows: d1005, dpp699, p9p300. To add the 'd' and 'p' digits, use the usual number manipulation rules. ▪ To use this feature with FXO interfaces, configure the device to operate in one-stage dialing mode. ▪ 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 IsWaitForDialTone (configurable for the entire device) is ignored. ▪ The FXS interface send SIP 200 OK responses only after the DTMF dialing is complete. ▪ This parameter can also be configured per Tel Profile, using the TelProfile parameter.
Web/EMS: RFC 2833 Payload Type **[RFC2833PayloadType]**	The 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. **Notes:** ▪ Certain vendors (e.g., Cisco) use payload type 101 for RFC 2833. ▪ 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.
[ReplaceNumberSignWithEscapeChar]	Determines whether to replace the number sign (#) with the escape character (%23) in outgoing SIP messages for Tel-to-IP calls. ▪ **[0]** Disable (default) ▪ **[1]** 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. **Note:** This parameter is applicable only if the parameter IsSpecialDigits is set 1.
Web: Special Digit Representation EMS: Use Digit For Special DTMF **[UseDigitForSpecialDTMF]**	Defines the representation for 'special' digits ('*' and '#') that are used for out-of-band DTMF signaling (using SIP INFO/NOTIFY). ▪ **[0]** Special = Uses the strings '*' and '#' (default). ▪ **[1]** Numeric = Uses the numerical values 10 and 11.

10.12.3 Digit Collection and Dial Plan Parameters

The digit collection and dial plan parameters are described in the table below.

Table 10-38: Digit Collection and Dial Plan Parameters

Parameter	Description
Web/EMS: Dial Plan Index **[DialPlanIndex]**	Determines 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. 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. **Notes:** ▪ If this parameter is configured to select a Dial Plan index, the settings of the parameter DigitMapping are ignored. ▪ 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. ▪ This parameter can also be configured per Tel Profile, using the TelProfile parameter. ▪ For a detailed description of the Dial Plan file, see "External Dial Plan File" on page 230.
[Tel2IPSourceNumberMappingDialPlanIndex]	Defines the Dial Plan index in the external Dial Plan file for the Tel-to-IP Source Number Mapping feature. The valid value range is 0 to 7, defining the Dail Plan index **[Plan x]** in the Dial Plan file. The default is -1 (disabled). For a detailed description of this feature, see Modifying ISDN-to-IP Calling Party Number.
Web: Digit Mapping Rules EMS: Digit Map Pat terns **[DigitMapping]**	Defines the digit map pattern. 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. 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: ▪ **[n-m]:** Range of numbers (not letters). ▪ **.** (single dot): Repeat digits until next notation (e.g., T). ▪ **x:** Any single digit. ▪ **T:** Dial timeout (configured by the TimeBetweenDigits parameter). ▪ **S:** 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

Parameter	Description
	can enter the digit 8. An example of a digit map is shown below: 11xS|00T|[1-7]xxx|8xxxxxxx|#xxxxxxx|*xx|91xxxxxxxxxx|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.'). **Notes:** ▪ 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. ▪ For a detailed description of digit mapping, see "Digit Mapping" on page 229.
Web: Max Digits in Phone Num EMS: Max Digits in Phone Number **[MaxDigits]**	Defines the maximum number of collected destination number digits that can be received (i.e., dialed) from the Tel side. When the number of collected digits reaches this maximum, the device uses these digits for the called destination number. The valid range is 1 to 49. The default value is 5. **Notes:** ▪ Instead of using this parameter, Digit Mapping rules can be configured. ▪ Dialing ends when any of the following scenarios occur: ✓ Maximum number of digits is dialed ✓ Interdigit Timeout (TimeBetweenDigits) expires ✓ Pound (#) key is pressed ✓ Digit map pattern is matched
Web: Inter Digit Timeout for Overlap Dialing **[sec]** EMS: Interdigit Timeout (Sec) **[TimeBetweenDigits]**	Defines the time (in seconds) that the device waits between digits that are dialed by the user. When this inter-digit timeout expires, the device uses the collected digits to dial the called destination number. The valid range is 1 to 10. The default value is 4.
Web: Enable Special Digits EMS: Use '#' For Dial Termination **[IsSpecialDigits]**	Determines whether the asterisk (*) and pound (#) digits can be used in DTMF. ▪ **[0]** Disable = Use '*' or '#' to terminate number collection (refer to the parameter UseDigitForSpecialDTMF). (Default.) ▪ **[1]** Enable = Allows '*' and '#' for telephone numbers dialed by a user or for the endpoint telephone number. **Note:** These symbols can always be used as the first digit of a dialed number even if you disable this parameter.

10.12.4 Voice Mail Parameters

The voice mail parameters are described in the table below. For detailed information on the Voice Mail application, refer to the *CPE Configuration Guide for Voice Mail*.

Note: Voice Mail is applicable only to FXO interfaces.

Table 10-39: Voice Mail Parameters

Parameter	Description
Web/EMS: Voice Mail Interface **[VoiceMailInterface]**	Enables the device's Voice Mail application and determines the communication method used between the PBX and the device. ▪ **[0]** None (default) ▪ **[1]** DTMF ▪ **[2]** SMDI **Note:** To enable voice mail per Hunt Group, you can use a Tel Profile ID (using the TelProfile parameter) that is configured with voice mail interface enabled. This eliminates the phenomenon of call delay on lines not implementing voice mail when voice mail is enabled using this global parameter.
Web: Enable VoiceMail URI EMS: Enable VMURI **[EnableVMURI]**	Enables or disables the interworking of target and cause for redirection from Tel to IP and vice versa, according to RFC 4468. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Enable = Enable
Web/EMS: Line Transfer Mode **[LineTransferMode]**	Determines the call transfer method used by the device. ▪ **[0]** None = IP (default). ▪ **[1]** Blind = PBX blind transfer. After receiving a REFER message from the IP side, the FXO sends a hook-flash to the PBX, dials the digits (that are received in the Refer-To header), and then immediately drops the line (on-hook). The PBX performs the transfer internally. ▪ **[2]** Semi Supervised = PBX Semi-Supervised transfer. After receiving a REFER message from the IP side, the FXO 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 approximately 2 seconds), the device completes the call transfer by releasing the line; otherwise, 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 towards the FXO line to restore connection to the original call. ▪ **[3]** Supervised = PBX Supervised transfer. After receiving a REFER message from the IP side, the FXO sends a hook-flash to the PBX, and then dials the digits

Parameter	Description
	(that are received in the Refer-To header). The FXO waits for connection of the transfer call and if speech is detected (e.g., "hello") within approximately 2 seconds, the device completes the call transfer by releasing the line; otherwise, 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 towards the FXO line to restore connection to the original call.
SMDI Parameters	
Web/EMS: Enable SMDI **[SMDI]**	Enables Simplified Message Desk Interface (SMDI) interface on the device. ▪ **[0]** Disable = Normal serial (default) ▪ **[1]** Enable (Bellcore) ▪ **[2]** Ericsson MD-110 ▪ **[3]** NEC (ICS) **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ 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).
Web/EMS: SMDI Timeout **[SMDITimeOut]**	Determines 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. 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. The valid range is 0 to 10000 (i.e., 10 seconds). The default value is 2000.
Message Waiting Indication (MWI) Parameters	
Web: MWI Off Digit Pattern EMS: MWI Off Code **[MWIOffCode]**	Determines the digit code used by the device to notify the PBX that there aren't any messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string.
Web: MWI On Digit Pattern EMS: MWI On Code **[MWIOnCode]**	Determines 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. The valid range is a 25-character string.
Web: MWI Suffix Pattern EMS: MWI Suffix Code **[MWISuffixCode]**	Determines 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.

Parameter	Description
Web: MWI Source Number EMS: MWI Source Name **[MWISourceNumber]**	Determines 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.
Digit Patterns 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 *CPE Configuration Guide for Voice Mail*.	
Web: Forward on Busy Digit Pattern (Internal) EMS: Digit Pattern Forward On Busy **[DigitPatternForwardOnBusy]**	Determines 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.
Web: Forward on No Answer Digit Pattern (Internal) EMS: Digit Pattern Forward On No Answer **[DigitPatternForwardOnNoAnswer]**	Determines 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 **[DigitPatternForwardOnDND]**	Determines 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 **[DigitPatternForwardNoReason]**	Determines 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 **[DigitPatternForwardOnBusyExt]**	Determines 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 **[DigitPatternForwardOnNoAnswerExt]**	Determines 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 **[DigitPatternForwardOnDNDExt]**	Determines 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.
Web: Forward on No Reason Digit Pattern (External) EMS: VM Digit Pattern No Reason External **[DigitPatternForwardNoReasonExt]**	Determines 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 **[DigitPatternInternalCall]**	Determines 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 **[DigitPatternExternalCall]**	Determines the digit pattern used by the PBX to indicate an external call. The valid range is a 120-character string.

Parameter	Description
Web: Disconnect Call Digit Pattern EMS: Tel Disconnect Code **[TelDisconnectCode]**	Determines 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 **[DigitPatternDigitToIgnore]**	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.

10.12.5 Supplementary Services Parameters

This subsection describes the device's supplementary telephony services parameters.

10.12.5.1 Caller ID Parameters

The caller ID parameters are described in the table below.

Table 10-40: Caller ID Parameters

Parameter	Description
Web: Caller ID Permissions Table **EMS: SIP Endpoints > Caller ID**	
[EnableCallerID]	This ini file table parameter configures Caller ID permissions. It allows you to enable or disable (per port) Caller ID generation (for FXS interfaces) and detection (for FXO interfaces). The format of this parameter is as follows: [EnableCallerID] FORMAT EnableCallerID_Index = EnableCallerID_IsEnabled; [\EnableCallerID] Where, ▪ Index = Port number (where 0 depicts Port 1). ▪ IsEnabled: ✓ **[0]** Disable = disables Caller ID (default). ✓ **[1]** Enable = enables Caller ID generation (FXS) or detection (FXO). For example: EnableCallerID 0 = 1; (caller ID enabled on Port 1) EnableCallerID 1 = 0; (caller ID disabled on Port 2) **Notes:** ▪ If a port is not configured, its Caller ID generation/detection is determined according to the global parameter EnableCallerID. ▪ For configuring this table using the Web interface, see Configuring Caller ID Permissions on page 158. ▪ For an explanation on using ini file table parameters, see Configuring ini File Table Parameters on page 194.
Web: Caller Display Information Table **EMS: SIP Endpoints > Caller ID**	
[CallerDisplayInfo]	This ini file table parameter enables the device to send Caller ID information to IP when a call is made. The called party can use this information for caller identification. The information

Parameter	Description
	configured in this table is sent in the SIP INVITE message's From header. The format of this parameter is as follows: [CallerDisplayInfo] FORMAT CallerDisplayInfo_Index = CallerDisplayInfo_DisplayString, CallerDisplayInfo_IsCidRestricted; [\CallerDisplayInfo] Where, ▪ Index = Port number (where 0 depicts Port 1). ▪ DisplayString = Caller ID string (up to 18 characters). ▪ IsCidRestricted = ✓ **[0]** Allowed = sends the defined caller ID string when a Tel-to-IP call is made using the corresponding device port (default). ✓ **[1]** Restricted = does not send the defined caller ID string. For example: CallerDisplayInfo 0 = Susan C.,0; ("Susan C." is sent as the Caller ID for Port 1) CallerDisplayInfo 1 = Mark M.,0; ("Mark M." is sent as Caller ID for Port 2) **Notes:** ▪ When FXS ports receive 'Private' or 'Anonymous' strings in the SIP From header, the calling name or number is not sent to the Caller ID display. ▪ If the Caller ID name is detected on an FXO line (the parameter EnableCallerID is set to 1), it is used instead of the Caller ID name defined in this table parameter. ▪ When the parameter CallerDisplayInfo_IsCidRestricted is set to 1 (Restricted), the Caller ID is sent to the remote side using only the SIP headers P-Asserted-Identity and P-Preferred-Identity (AssertedIdMode). ▪ To maintain backward compatibility, when the strings 'Private' or 'Anonymous' are entered in the parameter CallerDisplayInfo_DisplayString, the Caller ID is restricted and the value of the parameter CallerDisplayInfo_IsCidRestricted is ignored. ▪ The value of the parameter CallerDisplayInfo_IsCidRestricted is overridden by the parameter SourceNumberMapIp2Tel_IsPresentationRestricted in the 'Source Number Manipulation' table (table parameter SourceNumberMapIP2Tel). ▪ For configuring this table using the Web interface, see Configuring Caller Display Information on page 155. ▪ For an explanation on using ini file table parameters, see Configuring ini File Table Parameters on page 194.
Web/EMS: Enable Caller ID **[EnableCallerID]**	Determines whether Caller ID is enabled. ▪ **[0]** Disable = Disable the Caller ID service (default). ▪ **[1]** Enable = Enable the Caller ID service. If the Caller ID service is enabled, then for FXS interfaces,

Parameter	Description
	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 155. To disable/enable caller ID generation per port, see Configuring Call Forward on page 157.
Web: Caller ID Type EMS: Caller id Types **[CallerIDType]**	Defines one of the following standards for detection (FXO) and generation (FXS) of Caller ID, and detection (FXO) generation (FXS) of MWI (when specified) signals: ▪ **[0]** Standard Bellcore = Caller ID and MWI (default) ▪ **[1]** Standard ETSI = Caller ID and MWI ▪ **[2]** Standard NTT ▪ **[4]** Standard BT = Britain ▪ **[16]** Standard DTMF Based ETSI ▪ **[17]** Standard Denmark = Caller ID and MWI ▪ **[18]** Standard India ▪ **[19]** Standard Brazil **Notes:** ▪ 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, configure the parameter RingsBeforeCallerID to 0). ▪ Caller ID detection for Britain **[4]** is not supported on the device's FXO ports. Only FXS ports can generate the Britain **[4]** Caller ID. ▪ To select the Bellcore Caller ID sub standard, use the parameter BellcoreCallerIDTypeOneSubStandard. To select the ETSI Caller ID substandard, use the parameter ETSICallerIDTypeOneSubStandard. ▪ To select the Bellcore MWI sub standard, use the parameter BellcoreVMWITypeOneStandard. To select the ETSI MWI sub standard, use the parameter ETSIVMWITypeOneStandard. ▪ If you define Caller ID Type as NTT **[2],** you need to define the NTT DID signaling form (FSK or DTMF) using the parameter NTTDIDSignallingForm.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Web: Enable FXS Caller ID Category Digit For Brazil Telecom
[AddCPCPrefix2BrazilCallerID]</td><td>Enables the interworking of Calling Party Category (cpc) code from SIP INVITE messages to FXS Caller ID first digit.
▪ [0] Disable (default)
▪ [1] Enable = Interworking of CPC is performed
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 From (or P-Asserted-Id) header:
From:<sip:+551137077801;cpc=payphone@10.20.7.35>;tag=53700
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.
If the incoming INVITE message doesn't contain the 'cpc' parameter, nothing is added to the Caller ID number.
<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>
Notes:
▪ This parameter is applicable only to FXS interfaces.
▪ For this parameter to be enabled, you must also set the parameter EnableCallingPartyCategory to 1.</td></tr>
<tr><td>[EnableCallerIDTypeTwo]</td><td>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.
▪ [0] = Caller ID type 2 isn't played.
▪ [1] = Caller ID type 2 is played (default).</td></tr>
</table>

Parameter	Description
EMS: Caller ID Timing Mode **[AnalogCallerIDTimingMode]**	Determines when Caller ID is generated. ▪ **[0]** = Caller ID is generated between the first two rings (default). ▪ **[1]** = The device attempts to find an optimized timing to generate the Caller ID according to the selected Caller ID type. **Notes:** ▪ This parameter is applicable only to FXS interfaces. ▪ If this parameter is set to 1 and used with distinctive ringing, the Caller ID signal doesn't change the distinctive ringing timing. ▪ For this parameter to take effect, a device reset is required.
EMS: Bellcore Caller ID Type One Sub Standard **[BellcoreCallerIDTypeOneSubStandard]**	Selects the Bellcore Caller ID sub-standard. ▪ **[0]** = Between rings (default). ▪ **[1]** = Not ring related. **Note:** For this parameter to take effect, a device reset is required.
EMS: ETSI Caller ID Type One Sub Standard **[ETSICallerIDTypeOneSubStandard]**	Selects the ETSI FSK Caller ID Type 1 sub-standard (FXS only). ▪ **[0]** = ETSI between rings (default). ▪ **[1]** = ETSI before ring DT_AS. ▪ **[2]** = ETSI before ring RP_AS. ▪ **[3]** = ETSI before ring LR_DT_AS. ▪ **[4]** = ETSI not ring related DT_AS. ▪ **[5]** = ETSI not ring related RP_AS. ▪ **[6]** = ETSI not ring related LR_DT_AS. **Note:** For this parameter to take effect, a device reset is required.
Web: Asserted Identity Mode EMS: Asserted ID Mode **[AssertedIdMode]**	Determines whether the SIP header P-Asserted-Identity or P-Preferred-Identity is used in the generated INVITE request for Caller ID (or privacy). ▪ **[0]** Disabled = None (default) ▪ **[1]** Adding PAsserted Identity ▪ **[2]** Adding PPreferred Identity This parameter determines the header (P-Asserted-Identity or P-Preferred-Identity) used in the generated INVITE request. The header also depends on the calling Privacy (allowed or restricted). These headers are used to present the originating party's Caller ID. The Caller ID is composed of a Calling Number and (optionally), a Calling Name. 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 Tel or configured in the device), the From header is set to <anonymous@anonymous.invalid>.

Parameter	Description
Web: Use Destination As Connected Number **[UseDestinationAsConnectedNumber]**	Determines whether the device includes 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. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Notes:** ▪ 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 1. ▪ This parameter is applicable to FXO interfaces.
Web: Caller ID Transport Type EMS: Transport Type **[CallerIDTransportType]**	Determines the device's behavior for Caller ID detection. ▪ **[0]** Disable = The caller ID signal is not detected - DTMF digits remain in the voice stream. ▪ **[1]** Relay = (Currently not applicable.) ▪ **[3]** Mute = The caller ID signal is detected from the Tel side and then erased from the voice stream (default). **Note:** Caller ID detection is applicable only to FXO interfaces.

10.12.5.2 Call Waiting Parameters

The call waiting parameters are described in the table below.

Table 10-41: Call Waiting Parameters

Parameter	Description
Web/EMS: Enable Call Waiting **[EnableCallWaiting]**	Determines whether Call Waiting is enabled. ▪ **[0]** Disable = Disable the Call Waiting service. ▪ **[1]** Enable = Enable the Call Waiting service (default). 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. **Notes:** ▪ The device's Call Progress Tones (CPT) file must include a Call Waiting Ringback tone (caller side) and a Call Waiting tone (called side, FXS only). ▪ The EnableHold parameter must be enabled on both the calling and the called side. ▪ You can use the ini file table parameter CallWaitingPerPort to enable Call Waiting per port. ▪ For information on the Call Waiting feature, see "Call Waiting" on page 261. ▪ For information on the Call Progress Tones file, see Configuring the Call Progress Tones File.

Parameter	Description
EMS: Send 180 For Call Waiting **[Send180ForCallWaiting]**	Determines the SIP response code for indicating Call Waiting. ▪ **[0]** = Use 182 Queued response to indicate call waiting (default). ▪ **[1]** = Use 180 Ringing response to indicate call waiting.
Web: Call Waiting Table **EMS: SIP Endpoints > Call Waiting**	
[CallWaitingPerPort]	This ini file table parameter configures call waiting per FXS port. The format of this parameter is as follows: [CallWaitingPerPort] FORMAT CallWaitingPerPort_Index = CallWaitingPerPort_IsEnabled; [\CallWaitingPerPort] Where, ▪ Index = port number (where 0 denotes Port 1). ▪ IsEnabled: ✓ **[0]** Disable = no call waiting for the specific port. ✓ **[1]** Enable = enables call waiting for the specific port. When the FXS device receives a call on a busy endpoint (port), it responds with a SIP 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 initiates the waiting call plays a Call Waiting Ringback tone to the calling party after a 182 response is received. For example: CallWaitingPerPort 0 = 0; (call waiting disabled for Port 1) CallWaitingPerPort 1 = 1; (call waiting enabled for Port 2) **Notes:** ▪ This parameter is applicable only to FXS ports. ▪ You can configure up 8 table entries for MP-118 and up to 24 entries for MP-124. ▪ If this parameter is not configured (default), call waiting is determined according to the global parameter EnableCallWaiting. ▪ The device's CPT file 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 configuring this table using the Web interface, see Configuring Call Waiting on page 159. ▪ For a description on using ini file table parameters, see Configuring ini File Table Parameters on page 194.
Web: Number of Call Waiting Indications EMS: Call Waiting Number of Indications **[NumberOfWaitingIndications]**	Number of Call Waiting indications that are played to the called telephone that is connected to the device for Call Waiting. The valid range is 1 to 100 indications. The default value is 2. **Note:** This parameter is applicable only to FXS ports.

Parameter	Description
Web: Time Between Call Waiting Indications EMS: Call Waiting Time Between Indications **[TimeBetweenWaitingIndications]**	Time (in seconds) between consecutive call waiting indications for call waiting. The valid range is 1 to 100. The default value is 10. **Note:** This parameter is applicable only to FXS ports.
Web/EMS: Time Before Waiting Indications **[TimeBeforeWaitingIndication]**	Defines the interval (in seconds) before a call waiting indication is played to the port that is currently in a call. The valid range is 0 to 100. The default time is 0 seconds. **Note:** This parameter is applicable only to FXS ports.
Web/EMS: Waiting Beep Duration **[WaitingBeepDuration]**	Duration (in msec) of call waiting indications that are played to the port that is receiving the call. The valid range is 100 to 65535. The default value is 300. **Note:** This parameter is applicable only to FXS ports.
EMS: First Call Waiting Tone ID **[FirstCallWaitingToneID]**	Determines 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). There are three ways to use the distinctive call waiting tones: ▪ 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. ▪ Playing the call waiting tone according to PriorityIndex in the ToneIndex ini file table parameter. ▪ Playing the call waiting tone according to the parameter “CallWaitingTone#' of a SIP INFO message. The device plays the tone received in the 'play tone CallWaitingTone#' parameter of an INFO message plus the value of this parameter minus 1. The valid range is -1 to 1,000. The default value is -1 (i.e., not used). **Notes:** ▪ It is assumed that all Call Waiting Tones are defined in sequence in the CPT file. ▪ SIP Alert-Info header examples: ✓ Alert-Info:<Bellcore-dr2> ✓ Alert-Info:<http://…/Bellcore-dr2> (where "dr2" defines call waiting tone #2) ▪ The SIP INFO message is according to Broadsoft's application server definition. Below is an example of such an INFO message: INFO sip:06@192.168.13.2:5060 SIP/2.0 Via:SIP/2.0/UDP 192.168.13.40:5060;branch=z9hG4bK040066422630 From: <sip:4505656002@192.168.13.40:5060>;tag=1455352915 To: <sip:06@192.168.13.2:5060> Call-ID:0010-0008@192.168.13.2 CSeq:342168303 INFO Content-Length:28 Content-Type:application/broadsoft play tone CallWaitingTone1

10.12.5.3 Call Forwarding Parameters

The call forwarding parameters are described in the table below.

Table 10-42: Call Forwarding Parameters

Parameter	Description
Web: Enable Call Forward **[EnableForward]**	Determines whether Call Forward is enabled. ▪ **[0]** Disable = Disable the Call Forward service. ▪ **[1]** Enable = Enable Call Forward service (using REFER) (default). For FXS interfaces, the 'Call Forward' table (FwdInfo parameter) must be defined to use the Call Forward service. **Note:** To use this service, the devices at both ends must support this option.
Web: Call Forwarding Table **EMS: SIP Endpoints > Call Forward**	
[FwdInfo]	This ini file table parameter forwards (redirects) 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. The format of this parameter is as follows: [FwdInfo] FORMAT FwdInfo_Index = FwdInfo_Type, FwdInfo_Destination, FwdInfo_NoReplyTime; [\FwdInfo] Where, ▪ Index = Port number (where 0 depicts Port 1). ▪ Type = the scenario for forwarding the call: ✓ **[0]** Deactivate = Don't forward incoming calls (default). ✓ **[1]** On Busy = Forward incoming calls when the port is busy. ✓ **[2]** Unconditional = Always forward incoming calls. ✓ **[3]** No Answer = Forward incoming calls that are not answered within the time specified in the 'Time for No Reply Forward' field. ✓ **[4]** 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. ✓ **[5]** Do Not Disturb = Immediately reject incoming calls. ▪ Destination = Telephone number or URI (<number>@<IP address>) to where the call is forwarded. ▪ NoReplyTime = Timeout (in seconds) for No Reply. If you have set the Forward Type for this port to No Answer **[3],** enter the number of seconds the device waits before forwarding the call to the specified phone number. For example: ▪ Below configuration forwards calls originally destined to Port 1 to "1001" upon On Busy: FwdInfo 0 = 1,1001,30; ▪ Below configuration forwards calls originally destined to Port 2 to an IP address upon On Busy: FwdInfo 1 = 1,2003@10.5.1.1,30; **Notes:** ▪ Ensure that the Call Forward feature is enabled (default) for the settings of this table parameter to take effect. To enable Call

Parameter	Description
	Forwarding, use the parameter EnableForward. ▪ If the parameter FwdInfo_Destination only contains a telephone number and a Proxy isn't used, the 'forward to' phone number must be specified in the 'Tel to IP Routing' (Prefix ini file parameter). ▪ For configuring this table using the Web interface, see Configuring Call Forward on page 157. ▪ For an explanation on using ini file table parameters, see Configuring ini File Table Parameters on page 194.
Call Forward Reminder Ring Parameters **Notes:** ▪ These parameters are applicable only to FXS interfaces. ▪ For a description of this feature, see Call Forward Reminder Ring on page 260.	
Web: Enable NRT Subscription **[EnableNRTSubscription]**	Enables Endpoint subscription for Ring reminder event notification feature. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Web: AS Subscribe IPGroupID **[ASSubscribeIPGroupID]**	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 **[NRTRetrySubscriptionTime]**	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: Call Forward Ring Tone ID **[CallForwardRingToneID]**	Defines the ringing tone type played when call forward notification is accepted. The valid value range is 1 to 5. The default is 1.

10.12.5.4 Message Waiting Indication Parameters

The message waiting indication (MWI) parameters are described in the table below.

Table 10-43: MWI Parameters

Parameter	Description
Web: Enable MWI EMS: MWI Enable **[EnableMWI]**	Enables Message Waiting Indication (MWI). ▪ **[0]** Disable = Disabled (default). ▪ **[1]** Enable = MWI service is enabled. **Notes:** ▪ This parameter is applicable only to FXS interfaces. ▪ The device supports only the receipt of SIP MWI NOTIFY messages (the device doesn't generate these messages). ▪ For detailed information on MWI, see "Message Waiting Indication" on page 262.
Web/EMS: MWI Analog Lamp **[MWIAnalogLamp]**	Enables the visual display of MWI. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Enable = Enables visual MWI by supplying line voltage of approximately 100 VDC to activate the phone's lamp. **Notes:** ▪ This parameter is applicable only for FXS interfaces. ▪ This parameter can also be configured per Tel Profile (using the TelProfile parameter).
Web/EMS: MWI Display **[MWIDisplay]**	Determines whether MWI information is sent to the phone display. ▪ **[0]** Disable = MWI information isn't sent to display (default). ▪ **[1]** Enable = The device generates an MWI message (determined by the parameter CallerIDType), which is displayed on the MWI display. **Note:** ▪ This parameter is applicable only to FXS interfaces. ▪ This parameter can also be configured per Tel Profile (using the TelProfile parameter).
Web: Subscribe to MWI EMS: Enable MWI Subscription **[EnableMWISubscription]**	Enables subscription to an MWI server. ▪ **[0]** No = Disables MWI subscription (default). ▪ **[1]** Yes = Enables subscription to an MWI server (defined by the parameter MWIServerIP address). **Note:** To configure whether the device subscribes per endpoint or per the entire device, use the parameter SubscriptionMode.
Web: MWI Server IP Address EMS: MWI Server IP **[MWIServerIP]**	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.

Parameter	Description
Web/EMS: MWI Server Transport Type **[MWIServerTransportType]**	Determines the transport layer used for outgoing SIP dialogs initiated by the device to the MWI server. ▪ **[-1]** Not Configured (default) ▪ **[0]** UDP ▪ **[1]** TCP ▪ **[2]** TLS **Note:** When set to 'Not Configured', the value of the parameter SIPTransportType is used.
Web: MWI Subscribe Expiration Time EMS: MWI Expiration Time **[MWIExpirationTime]**	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 **[SubscribeRetryTime]**	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 **[SubscriptionMode]**	Determines the method the device uses to subscribe to an MWI server. ▪ **[0]** Per Endpoint = Each endpoint subscribes separately - typically used for FXS interfaces (default). ▪ **[1]** Per Gateway = Single subscription for the entire device - typically used for FXO interfaces.
EMS: ETSI VMWI Type One Standard **[ETSIVMWITypeOneStandard]**	Selects the ETSI Visual Message Waiting Indication (VMWI) Type 1 sub-standard. ▪ **[0]** = ETSI VMWI between rings (default) ▪ **[1]** = ETSI VMWI before ring DT_AS ▪ **[2]** = ETSI VMWI before ring RP_AS ▪ **[3]** = ETSI VMWI before ring LR_DT_AS ▪ **[4]** = ETSI VMWI not ring related DT_AS ▪ **[5]** = ETSI VMWI not ring related RP_AS ▪ **[6]** = ETSI VMWI not ring related LR_DT_AS **Note:** For this parameter to take effect, a device reset is required.
EMS: Bellcore VMWI Type One Standard **[BellcoreVMWITypeOneStandard]**	Selects the Bellcore VMWI sub-standard. ▪ **[0]** = Between rings (default). ▪ **[1]** = Not ring related. **Note:** For this parameter to take effect, a device reset is required.

10.12.5.5 Call Hold Parameters

The call hold parameters are described in the table below.

Table 10-44: Call Hold Parameters

Parameter	Description
Web/EMS: Enable Hold **[EnableHold]**	Allows users (connected to the device) to place a call on hold. ▪ **[0]** Disable = Disables the Hold service ▪ **[1]** Enable = Enables the Hold service (default) If the Hold service is enabled, a user can place the call on hold (or remove from hold) using the Hook Flash button. On receiving a Hold request, the remote party is placed on hold and hears the hold tone. **Notes:** ▪ To use this service, the devices at both ends must support this option. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Web/EMS: Hold Format **[HoldFormat]**	Determines the format of the SDP in the Re-INVITE hold request. ▪ **[0]** 0.0.0.0 = The SDP "c=" field contains the IP address "0.0.0.0" and the "a=inactive" attribute (default). ▪ **[1]** Send Only = The SDP "c=" field contains the device's IP address and the "a=sendonly" attribute. **Note:** The device does not send any RTP packets when it is in hold state (for both hold formats).
Web/EMS:Held Timeout **[HeldTimeout]**	Determines 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). ▪ **[-1]** = The call is placed on hold indefinitely until the initiator of the on hold retrieves the call again (default). ▪ **[0 - 2400]** = Time to wait (in seconds) after which the call is released.
Web: Call Hold Reminder Ring Timeout EMS: CHRR Timeout **[CHRRTimeout]**	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. The valid range is 0 to 600. The default value is 30. **Notes:** ▪ This parameter is applicable only to FXS interfaces. ▪ This Reminder Ring feature can be disabled using the DisableReminderRing parameter.

Parameter	Description
[DisableReminderRing]	Disables the reminder ring, which notifies the FXS user of a call on hold or a waiting call when the phone is returned to on-hook position. ▪ **[0]** = (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. ▪ **[1]** = 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). **Note:** This parameter is applicable only to FXS interfaces.
[PlayDTMFduringHold]	Enables playing DTMF signals to the Tel side when a call is on hold. ▪ **[0]** = Disable (default) - if the call is in Hold (inactive) state, the device does not play DTMF signals to the Tel if it receives SIP INFO DTMF messages. ▪ **[1]** = Enable - the device stops playing the Held tone (if it was played) and starts playing DTMF digits according to received SIP INFO message(s). (The stopped Held tone is not played again.)

10.12.5.6 Call Transfer Parameters

The call transfer parameters are described in the table below.

Table 10-45: Call Transfer Parameters

Parameter	Description
Web/EMS: Enable Transfer **[EnableTransfer]**	Determines whether call transfer is enabled. ▪ **[0]** Disable = Disable the call transfer service. ▪ **[1]** Enable = Enable the call transfer service (using REFER)(default). 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. **Notes:** ▪ To use call transfer, the devices at both ends must support this option. ▪ To use call transfer, set the parameter EnableHold to 1.
Web: Transfer Prefix EMS: Logical Prefix For Transferred Call **[xferPrefix]**	Defines the string that is added as a prefix to the transferred/forwarded called number when the REFER/3xx message is received. **Notes:** ▪ 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. ▪ This parameter can be used to apply different manipulation rules to differentiate transferred/forwarded number from the originally dialed number.

Parameter	Description
Web: Transfer Prefix IP 2 Tel **[XferPrefixIP2Tel]**	Defines the prefix that is added to the destination number received in the SIP Refer-To header (for IP-to-Tel calls). This parameter is applicable to FXO Blind Transfer modes (LineTransferMode = 1, 2 or 3). The valid range is a string of up to 9 characters. The default is an empty string.
Web/EMS: Enable Semi-Attended Transfer **[EnableSemiAttendedTransfer]**	Determines the device behavior when Transfer is initiated while in Alerting state. ▪ **[0]** Disable = Send REFER with the Replaces header (default). ▪ **[1]** Enable = Send CANCEL, and after a 487 response is received, send REFER without the Replaces header.
EMS: Blind Transfer Add Prefix **[KeyBlindTransferAddPrefix]**	Determines whether the device adds the Blind Transfer code (KeyBlindTransfer) to the dialed destination number. ▪ **[0]** Disable (default). ▪ **[1]** Enable.
EMS: Blind Transfer Disconnect Timeout **[BlindTransferDisconnectTimeout]**	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. The valid range is 0 to 1,000,000. The default is 0.

10.12.5.7 Three-Way Conferencing Parameters

The three-way conferencing parameters are described in the table below.

Table 10-46: Three-Way Conferencing Parameters

Parameter	Description
Web: Enable 3-Way Conference EMS: Enable 3 Way **[Enable3WayConference]**	Enables or disables the 3-Way Conference feature. ▪ **[0]** Disable = Disable (default) ▪ **[1]** Enable = Enables 3-way conferencing **Note:** For this parameter to take effect, a device reset is required.
Web: 3-Way Conference Mode EMS: 3 Way Mode **[3WayConferenceMode]**	Defines the mode of operation when the 3-Way Conference feature is used. ▪ **[0]** AudioCodes 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. This conference mode is used when operating with AudioCodes IPMedia conferencing server. (Default) ▪ **[1]** 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

Parameter	Description

	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.
	▪ **[2]** On Board = On-board three-way conference. The conference is established on the device without the need of an external Conference server. The device utilizes resources from idle ports to establish the conference call. You can limit the number of simultaneous, on-board 3-way conference calls, by using the MaxInBoardConferenceCalls parameter. In addition, you can designate ports that can't be used as a resource for on-board, conference calls initiated by other ports, using the 3WayConfNoneAllocateablePorts parameter.
	Notes:
	▪ This parameter is applicable only to FXS interfaces.
	▪ When using an external conference server (i.e., options **[0]** or **[1]),** more than one three-way conference may be supported (up to six).
	▪ Currently, the on-board 3-way conference mode (option 2) is not supported when using SRTP.
	▪ For local, onboard three-way conferencing (option **[2])** on MP-112, the following additional parameter settings must be made:
	EnableIPMediaChannels = 1
	`[ IPMediaChannels ]`
	`FORMAT IPMediaChannels_Index = IPMediaChannels_ModuleID, IPMediaChannels_DSPChannelsReserved;`
	`IPMediaChannels 0 = 1, 2;`
	`[ \IPMediaChannels ]`

Web: Max 3 Way Conference On Board Calls EMS: Max In Board Calls **[MaxInBoardConferenceCalls]**	Determines the maximum number of simultaneous, on-board three-way conference calls. The valid range is 0 to 2. The default is 2. **Notes:** ▪ For enabling on-board, three-way conferencing, use the 3WayConferenceMode parameter. ▪ This parameter is applicable only to FXS interfaces.
Web: Three Way Conference Non Allocatable Ports EMS: Non Allocateable Port Number **[3WayConfNoneAllocateablePorts]**	Determines the ports that are not allocated as resources for on-board three-way conference calls that are initiated by other ports. Ports that are not configured with this parameter (and that are idle) are used by the device as a resource for establishing these type of conference calls. The valid range is up to 8 ports. To add a range of ports, use the comma separator. For example, for not allowing the use of ports 2, 4 and 8 as resources, enter the following value: 2,4,8. The order of the entered values is not relevant (i.e., the example above can be entered as 8,2,4). The default is 0. **Notes:** ▪ To enable on-board, three-way conferencing, use the 3WayConferenceMode and MaxInBoardConferenceCalls parameters. ▪ This parameter is applicable only to FXS interfaces.

Parameter	Description
Web: Establish Conference Code EMS: Establish Code **[ConferenceCode]**	Defines the digit pattern, which upon detection, generates the Conference-initiating INVITE when 3-way conferencing is enabled (Enable3WayConference is set to 1). The valid range is a 25-character string. The default is “!” (Hook-Flash).
Web/EMS: Conference ID **[ConferenceID]**	Defines the Conference Identification string (up to 16 characters). The default value is 'conf'. The device uses this identifier in the Conference-initiating INVITE that is sent to the media server when Enable3WayConference is set to 1. For example: ConferenceID = MyConference.

10.12.5.8 Emergency Call Parameters

The emergency call parameters are described in the table below.

Table 10-47: Emergency Call Parameters

Parameter	Description
Web/EMS: Emergency Numbers **[EmergencyNumbers]**	Defines a list of “emergency” numbers. 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. This scenario is applicable only to FXS interfaces. These emergency numbers can also be used for pre-emption of E911 IP-to-Tel calls when there are unavailable (busy) channels. In this scenario, the device terminates one of the busy channels and sends the E911 call to this channel. This feature is enabled by setting the CallPriorityMode parameter to 2 (“Emergency”) and by defining an emergency number value of “911” for the EmergencyNumbers parameter. For a description of this feature, see Pre-empting Existing Call for E911 IP-to-Tel Call. This scenario is applicable to FXS/FXO interface. The list can include up to four different numbers, where each number can be up to four digits long. Example: EmergencyNumbers = ‘100’,’911’,’112’
Web: Emergency Calls Regret Timeout EMS: Emergency Regret Timeout **[EmergencyRegretTimeout]**	Determines 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 value is 10. **Note:** This parameter is applicable only to FXS interfaces.

10.12.5.9 Call Cut-Through Parameters

The call cut-through parameters are described in the table below.

Table 10-48: Call Cut-Through Parameters

Parameter	Description
Web: Enable Calls Cut Through EMS: Cut Through **[CutThrough]**	Enables FXS endpoints to receive incoming IP calls while the port is in off-hook state. ▪ **[0]** Disable (default) ▪ **[1]** Enable 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. 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. The waiting call is automatically answered by the device when the current call is terminated (configured by setting the parameter EnableCallWaiting to 1). **Note:** This feature is applicable only to FXS interfaces.

10.12.5.10 Automatic Dialing Parameters

The automatic dialing upon off-hook parameters are described in the table below.

Table 10-49: Automatic Dialing Parameters

Parameter	Description
Web: Automatic Dialing Table **EMS: SIP Endpoints > Auto Dial**	
[TargetOfChannel]	This *ini* file table parameter defines telephone numbers that are automatically dialed when a specific FXS or FXO port is used (i.e., telephone is off-hooked). The format of this parameter is as follows: [TargetOfChannel] FORMAT TargetOfChannel_Index = TargetOfChannel_Destination, TargetOfChannel_Type, TargetOfChannel_HotLineToneDuration; [\TargetOfChannel] Where, ▪ Index = Port number (where 0 depicts Port 1). ▪ Destination = Destination phone number that you want dialed. ▪ Type: ✓ **[0]** Disable = automatic dialing is disabled. ✓ **[1]** Enable = Destination phone number is automatically dialed if phone is off-hooked (for FXS interface) or ring signal is applied to port (FXO interface). ✓ **[2]** Hotline = enables the Hotline feature where if the phone is off-hooked and no digit is pressed for a user-defined duration (configured by the parameter HotLineToneDuration), the destination phone number is automatically dialed.

Parameter	Description
	▪ HotLineToneDuration = if Hotline is enabled and the phone (connected to the specific port) is off-hooked and no digit is pressed for this user-defined duration (timeout), the device automatically initiates a call to the user-defined destination phone number. The value range is 0 to 60 seconds, with default as 16. Note that you can use the "global" HotLineToneDuration parameter to define this interval for all ports. For example, the below configuration defines automatic dialing of phone number 911 when the phone that is connected to Port 1 is off-hooked for over 10 seconds: TargetOfChannel 0 = 911, 1 ,10; (phone number "911" is automatically dialed for Port 1after being off-hooked for 10 seconds) **Notes:** ▪ This is parameter is applicable to FXS and FXO interfaces. ▪ The indexing of this *ini* file table parameter starts at 0. ▪ Define this parameter for each device port that implements Automatic Dialing. ▪ This parameter can appear up to 8 times for MP-118-port and up to 24 times for MP-124 devices. ▪ After a ring signal is detected on an 'Enabled' FXO port, the device initiates a call to the destination number without seizing the line. The line is seized only after the call is answered. After a ring signal is detected on a 'Disabled' or 'Hotline' FXO port, the device seizes the line. ▪ For configuring this table using the Web interface, see "Configuring Automatic Dialing" on page 154. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.12.5.11 Direct Inward Dialing Parameters

The Direct Inward Dialing (DID) parameters are described in the table below.

Table 10-50: DID Parameters

Parameter	Description
Web/EMS: Enable DID Wink **[EnableDIDWink]**	Enables Direct Inward Dialing (DID) using Wink-Start signaling. ▪ **[0]** Disable = Disables DID Wink(default). ▪ **[1]** Enable = Enables DID Wink. If enabled, the device can be used for connection to EIA/TIA-464B DID Loop Start lines. Both FXO (detection) and FXS (generation) are supported. An FXO interface dials DTMF digits after a Wink signal is detected (instead of a Dial tone). An FXS interface generates the Wink signal after the detection of off-hook (instead of playing a Dial tone). **Note:** This parameter can also be configured per Tel Profile, using the TelProfile parameter.
Web/EMS: Delay Before DID Wink **[DelayBeforeDIDWink]**	Defines the time interval (in msec) between detection of off-hook and generation of a DID Wink. The valid range is 0 to 1,000. The default value is 0. **Note:** This parameters is applicable only to FXS interfaces.

Parameter	Description
EMS: NTT DID Signalling Form **[NTTDIDSignallingForm]**	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. ▪ **[0]** = FSK-based signaling (default) ▪ **[1]** = DTMF-based signaling **Note:** This parameter is applicable only to FXS interfaces.
EMS: Enable DID **[EnableDID]**	This *ini* file 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. The format of this parameter is as follows: [EnableDID] FORMAT EnableDID_Index = EnableDID_IsEnable; [\EnableDID] Where, ▪ Index = Port number (where 0 denotes Port 1). ▪ IsEnable = Enables **[1]** or disables **[0]** (default) Japan NTT Modem DID support. For example: EnableDID 0 = 1; (DID is enabled on Port 1) **Notes:** ▪ This parameter is applicable only to FXS interfaces. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
[WinkTime]	Defines the time (in msec) elapsed between two consecutive polarity reversals. This parameter can be used for DID signaling. The valid range is 0 to 4,294,967,295. The default is 200. **Notes:** ▪ This parameter is applicable to FXS and FXO interfaces. ▪ For this parameter to take effect, a device reset is required.

10.12.5.12 MLPP Parameters

The Multilevel Precedence and Preemption (MLPP) parameters are described in the table below.

Table 10-51: MLPP Parameters

Parameter	Description
Web/EMS: Call Priority Mode **[CallPriorityMode]**	Enables priority call handling. ▪ **[0]** Disable = Disable (default). ▪ **[1]** 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 congestion occurs in a network. ▪ **[2]** 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 Hunt 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: ✓ 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".) ✓ The incoming SIP INVITE message contains the “emergency” value in the Priority header. **Notes:** ✓ Applicable to FXS/FXO interface. ✓ 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. ✓ For a detailed description, see Pre-empting Existing Call for E911 IP-to-Tel Call.
Web: MLPP DiffServ EMS: Diff Serv **[MLPPDiffserv]**	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 MLPP calls with the Resource-Priority header. The valid range is 0 to 63. The default value is 50. **Notes:** ▪ The same value must be configured for this parameter and the parameter PremiumServiceClassControlDiffServ. ▪ Outgoing calls are tagged according to the parameter PremiumServiceClassControlDiffServ.

Parameter	Description
EMS: E911 MLPP Behavior **[E911MLPPBehavior]**	Defines the E911 (or Emergency Telecommunication Services/ETS) MLPP Preemption mode: ▪ **[0]** Standard Mode - ETS calls have the highest priority and preempt any MLPP call (default). ▪ **[1]** Treat as routine mode - ETS calls are handled as routine calls.
Web/EMS: Precedence Ringing Type **[PrecedenceRingingType]**	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. The valid range is -1 to 16. The default value is -1 (i.e., plays standard Ringing tone).

Multiple Differentiated Services Code Points (DSCP) per MLPP Call Priority Level (Precedence) Parameters

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:

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 **[MLPPRoutineRTPDSCP]**	Defines the RTP DSCP for MLPP Routine precedence call level. The valid range is -1 to 63. The default is -1. **Note:** If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined for IP Profiles per call (using the parameter IPProfile).
Web/EMS: RTP DSCP for MLPP Priority **[MLPPPriorityRTPDSCP]**	Defines the RTP DSCP for MLPP Priority precedence call level. The valid range is -1 to 63. The default is -1. **Note:** If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined for IP Profiles per call (using the parameter IPProfile).
Web/EMS: RTP DSCP for MLPP Immediate **[MLPPImmediateRTPDSCP]**	Defines the RTP DSCP for MLPP Immediate precedence call level. The valid range is -1 to 63. The default is -1. **Note:** If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined for IP Profiles per call (using the parameter IPProfile).
Web/EMS: RTP DSCP for MLPP Flash **[MLPPFlashRTPDSCP]**	Defines the RTP DSCP for MLPP Flash precedence call level. The valid range is -1 to 63. The default is -1. **Note:** If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined for IP Profiles per call (using the parameter IPProfile).

Parameter	Description
Web/EMS: RTP DSCP for MLPP Flash Override **[MLPPFlashOverRTPDSCP]**	Defines the RTP DSCP for MLPP Flash-Override precedence call level. The valid range is -1 to 63. The default is -1. **Note:** If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined for IP Profiles per call (using the parameter IPProfile).
Web/EMS: RTP DSCP for MLPP Flash-Override-Override **[MLPPFlashOverOverRTPDSCP]**	Defines the RTP DSCP for MLPP Flash-Override-Override precedence call level. The valid range is -1 to 63. The default is -1. **Note:** If set to -1, the DiffServ value is taken from the global parameter PremiumServiceClassMediaDiffServ or as defined for IP Profiles per call (using the parameter IPProfile).

10.12.6 Answer and Disconnect Supervision Parameters

The answer and disconnect supervision parameters are described in the table below.

Table 10-52: Answer and Disconnect Parameters

Parameter	Description
Web: Answer Supervision EMS: Enable Voice Detection **[EnableVoiceDetection]**	Enables the sending of SIP 200 OK upon detection of speech, fax, or modem. ▪ **[1]** Yes = The device sends a SIP 200 OK (in response to an INVITE message) when speech, fax, or modem is detected. ▪ **[0]** No = The device sends a SIP 200 OK only after it completes dialing (default). 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. **Notes:** ▪ This feature is applicable only to one-stage dialing (FXO). ▪ This parameter is applicable only to FXO interfaces.
Web/EMS: Max Call Duration (min) **[MaxCallDuration]**	Defines the maximum call duration (in minutes). If this time expires, both sides of the call are released (IP and Tel). The valid range is 0 to 35,791. The default is 0 (i.e., no limitation).
Web/EMS: Disconnect on Dial Tone **[DisconnectOnDialTone]**	Determines whether the device disconnects a call when a dial tone is detected from the PBX. ▪ **[0]** Disable = Call is not released (default). ▪ **[1]** Enable = Call is released if dial tone is detected on the device's FXO port. **Notes:** ▪ This parameter is applicable only to FXO interfaces. ▪ This option is in addition to the mechanism that disconnects a call when either busy or reorder tones are detected.

Parameter	Description
Web: Send Digit Pattern on Connect EMS: Connect Code **[TelConnectCode]**	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. **Note:** This parameter is applicable to FXO.
Web: Disconnect on Broken Connection EMS: Disconnect Calls on Broken Connection **[DisconnectOnBrokenConnection]**	Determines whether the device releases the call if RTP packets are not received within a user-defined timeout. ▪ **[0]** No ▪ **[1]** Yes (default) **Notes:** ▪ The timeout is configured by the BrokenConnectionEventTimeout parameter. ▪ 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. ▪ 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. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Web: Broken Connection Timeout EMS: Broken Connection Event Timeout **[BrokenConnectionEventTimeout]**	The time period (in 100-msec units) after which a call is disconnected if an RTP packet is not received. The valid range is from 3 (i.e., 300 msec) to an unlimited value (e.g., 20 hours). The default value is 100 (i.e., 10000 msec or 10 seconds). **Notes:** ▪ This parameter is applicable only if the parameter DisconnectOnBrokenConnection is set to 1. ▪ Currently, this feature functions only if Silence Suppression is disabled.
Web: Disconnect Call on Silence Detection EMS: Disconnect On Detection Of Silence **[EnableSilenceDisconnect]**	Determines whether calls are disconnected after detection of silence. ▪ **[1]** Yes = The device disconnects calls in which silence occurs (in both call directions) for more than a user-defined time. ▪ **[0]** No = Call is not disconnected when silence is detected (default). The silence duration can be configured by the FarEndDisconnectSilencePeriod parameter (default 120). **Note:** To activate this feature, set the parameters EnableSilenceCompression and FarEndDisconnectSilenceMethod to 1.

Parameter	Description
Web: Silence Detection Period **[sec]** EMS: Silence Detection Time Out **[FarEndDisconnectSilencePeriod]**	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. **Note:** For this parameter to take effect, a device reset is required.
Web: Silence Detection Method **[FarEndDisconnectSilenceMethod]**	Silence detection method. ▪ **[0]** None = Silence detection option is disabled. ▪ **[1]** Packets Count = According to packet count. ▪ **[2]** Voice/Energy Detectors = According to energy and voice detectors (default). ▪ **[3]** All = According to packet count, and energy and voice detectors. **Note:** For this parameter to take effect, a device reset is required.
[FarEndDisconnectSilenceThreshold]	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%. **Notes:** ▪ This parameter is applicable only if silence is detected according to packet count (FarEndDisconnectSilenceMethod is set to 1). ▪ For this parameter to take effect, a device reset is required.
[BrokenConnectionDuringSilence]	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. ▪ **[0]** Disable (default). ▪ **[1]** Enable.
Web: Disconnect Call on Busy Tone Detection EMS: Disconnect On Detection End Tones **[DisconnectOnBusyTone]**	Determines whether a call is disconnected upon detection of a busy tone. ▪ **[0]** Disable = Do not disconnect call on detection of busy tone. ▪ **[1]** Enable = Call is released if busy or reorder (fast busy) tone is detected on the device's FXO port (default). **Notes:** ▪ This parameter is applicable only to FXO interfaces. ▪ This parameter can also be configured per Tel Profile, using the TelProfile parameter.

Parameter	Description
Polarity (Current) Reversal for Call Release (Analog Interfaces) Parameters	
Web: Enable Polarity Reversal EMS: Enable Reversal Polarity **[EnableReversalPolarity]**	Enables the polarity reversal feature for call release. ▪ **[0]** Disable = Disable the polarity reversal service (default). ▪ **[1]** Enable = Enable the polarity reversal service. 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. **Note:** This parameter can also be configured per Tel Profile, using the TelProfile parameter.
Web/EMS: Enable Current Disconnect **[EnableCurrentDisconnect]**	Enables call release upon detection of a Current Disconnect signal. ▪ **[0]** Disable = Disable the current disconnect service (default). ▪ **[1]** Enable = Enable the current disconnect service. If the current disconnect service is enabled: ▪ The FXO releases a call when a current disconnect signal is detected on its port. ▪ The FXS interface generates a 'Current Disconnect Pulse' after a call is released from IP. 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. **Note:** This parameter can also be configured per Tel Profile, using the TelProfile parameter.
EMS: Polarity Reversal Type **[PolarityReversalType]**	Defines the voltage change slope during polarity reversal or wink. ▪ **[0]** = Soft reverse polarity (default). ▪ **[1]** = Hard reverse polarity. **Notes:** ▪ This parameter is applicable only to FXS interfaces. ▪ 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). ▪ For this parameter to take effect, a device reset is required.

Parameter	Description
EMS: Current Disconnect Duration **[CurrentDisconnectDuration]**	The duration (in msec) of the current disconnect pulse. The range is 200 to 1500. The default is 900. **Notes:** ▪ This parameter is applicable for FXS and FXO interfaces. ▪ 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. ▪ For this parameter to take effect, a device reset is required.
[CurrentDisconnectDefaultThreshold]	Determines the line voltage threshold at which a current disconnect detection is considered. The valid range is 0 to 20 Volts. The default value is 4 Volts. **Notes:** ▪ This parameter is applicable only to FXO interfaces. ▪ For this parameter to take effect, a device reset is required.
[TimeToSampleAnalogLineVoltage]	Determines the frequency at which the analog line voltage is sampled (after offhook), for detection of the current disconnect threshold. The valid range is 100 to 2500 msec. The default value is 1000 msec. **Notes:** ▪ This parameter is applicable only to FXO interfaces. ▪ For this parameter to take effect, a device reset is required.

10.12.7 Tone Parameters

This subsection describes the device's tone parameters.

10.12.7.1 Telephony Tone Parameters

The telephony tone parameters are described in the table below.

Table 10-53: Tone Parameters

Parameter	Description
Web/EMS: Dial Tone Duration **[sec]** **[TimeForDialTone]**	Duration (in seconds) that the dial tone is played. 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. **Notes:** ▪ During play of dial tone, the device waits for DTMF digits. ▪ This parameter is not applicable when Automatic Dialing is enabled.
Web/EMS: Stutter Tone Duration **[StutterToneDuration]**	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. The range is 1,000 to 60,000. The default is 2,000 (i.e., 2 seconds). **Notes:** ▪ This parameter is applicable only to FXS interfaces. ▪ 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. ▪ The MWI tone takes precedence over the Call Forwarding Reminder tone. For detailed information on MWI, see Message Waiting Indication on page 262.
Web: FXO AutoDial Play BusyTone EMS: Auto Dial Play Busy Tone **[FXOAutoDialPlayBusyTone]**	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). ▪ **[0]** = Disable (default) ▪ **[1]** = Enable **Note:** This parameter is applicable only to FXO interfaces.

Parameter	Description
Web: Hotline Dial Tone Duration EMS: Hot Line Tone Duration **[HotLineToneDuration]**	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 154). The valid range is 0 to 60. The default is 16. **Notes:** ▪ This parameter is applicable to FXS and FXO interfaces. ▪ You can define the Hotline duration per FXS/FXO port using the Automatic Dialing table.
Web/EMS: Reorder Tone Duration **[sec]** **[TimeForReorderTone]**	The duration (in seconds) that the device plays a Busy or Reorder tone duration before releasing the line. The valid range is 0 to 254. The default is 0 seconds. Typically, after playing a Reorder/Busy tone for the specified duration, the device starts playing an Offhook Warning tone. **Notes:** ▪ The selection of Busy or Reorder tone is performed according to the release cause received from IP. ▪ This parameter can also be configured per Tel Profile, using the TelProfile parameter).
Web: Time Before Reorder Tone **[sec]** EMS: Time For Reorder Tone **[TimeBeforeReorderTone]**	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. The valid range is 0 to 60. The default is 0. **Note:** This parameter is applicable only to FXS interfaces.
Web: Cut Through Reorder Tone Duration **[sec]** **[CutThroughTimeForReOrderTone]**	Defines the duration (in seconds) of the Reorder tone played to the Tel 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. The valid values are 0 to 30. The default is 0 (i.e., no Reorder tone is played). **Note:** To enable the Cut-Through feature, use the CutThrough (for FXS channels) parameter.
Web/EMS: Enable Comfort Tone **[EnableComfortTone]**	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. ▪ **[0]** Disable (default) ▪ **[1]** Enable **Note:** This parameter is applicable to FXS and FXO interfaces.
[WarningToneDuration]	Defines the duration (in seconds) for which the Off-Hook Warning Tone is played to the user. The valid range is -1 to 2,147,483,647. The default is 600. **Note:** A negative value indicates that the tone is played infinitely.

Parameter	Description
Web: Play Ringback Tone to Tel EMS: Play Ring Back Tone To Tel **[PlayRBTone2Tel]**	Enables the play of the ringback tone (RBT) to the Tel side and determines the method for playing the RBT. ▪ **[0]** Don't Play = RBT is not played. ▪ **[1]** Play on Local = RBT is played to the Tel side of the call when a SIP 180/183 response is received. ▪ **[2]** Prefer IP = RBT is played 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 RBT (default). ▪ **[3]** Play Local Until Remote Media Arrive = Plays the RBT according to received media. The behaviour is similar to **[2].** 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 RBT if there are no prior received RTP packets. The device stops playing the local RBT 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 RBT.
Web: Play Ringback Tone to IP EMS: Play Ring Back Tone To IP **[PlayRBTone2IP]**	Determines whether or not the device plays a ringback tone (RBT) to the IP side for IP-to-Tel calls. ▪ **[0]** Don't Play = Ringback tone isn't played (default). ▪ **[1]** Play = Ringback tone is played after SIP 183 session progress response is sent. **Notes:** ▪ This parameter is applicable only to FXS interfaces. ▪ To enable the device to send a 183/180+SDP responses, set the EnableEarlyMedia parameter to 1. ▪ 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. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 122).
Tone Index Table	
[ToneIndex]	This ini file 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). This is based on calling number (source number prefix) and/or called (destination number/prefix) for IP-to-Tel calls. This allows different tones to be played for an FXS endpoint depending on the source or destination number of the IP-to-Tel call. The format of this parameter is as follows: [ToneIndex] FORMAT ToneIndex_Index = ToneIndex_FXSPort_First, ToneIndex_FXSPort_Last, ToneIndex_SourcePrefix, ToneIndex_DestinationPrefix, ToneIndex_PriorityIndex; [\ToneIndex] Where, ▪ FXSPort_First = starting range of FXS ports.

Parameter	Description
	▪ FXSPort_Last = end range of FXS ports. ▪ SourcePrefix = prefix of the calling number. ▪ DestinationPrefix = prefix of the called number. ▪ PriorityIndex = index for Distinctive Ringing and Call Waiting tones (default is 0): ✓ Ringing tone index = index in the CPT file for playing the ring tone. ✓ Call Waiting tone index = priority index + FirstCallWaitingToneID(*). For example, if you want to select the Call Waiting tone defined in the CPT file at Index #9, then you can enter 1 as the priority index and the value 8 for FirstCallWaitingToneID. The summation of these values equals 9, i.e., index #9. 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; **Notes:** ▪ You can define up to 50 indices. ▪ This parameter is applicable only to FXS interfaces. ▪ Typically, the Ringing and/or Call Waiting tone played is indicated in the SIP Alert-Info header field of the received INVITE message. If this header is not present, then the tone played is according to the settings of this table. ▪ For depicting a range of FXS ports, use the syntax x-y (e.g., "1-4" for ports 1 through 4). ▪ You can configure multiple entries with different source and/or destination prefixes and tones for the same FXS port.

10.12.7.2 Tone Detection Parameters

The signal tone detection parameters are described in the table below.

Table 10-54: Tone Detection Parameters

Parameter	Description
EMS: DTMF Enable **[DTMFDetectorEnable]**	Enables or disables the detection of DTMF signaling. ▪ **[0]** = Disable ▪ **[1]** = Enable (default)
EMS: MF R1 Enable **[MFR1DetectorEnable]**	Enables or disables the detection of MF-R1 signaling. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
EMS: User Defined Tone Enable **[UserDefinedToneDetectorEnable]**	Enables or disables the detection of User Defined Tones signaling, applicable for Special Information Tone (SIT) detection. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable

Parameter	Description
EMS: SIT Enable **[SITDetectorEnable]**	Enables or disables SIT detection according to the ITU-T recommendation E.180/Q.35. ▪ **[0]** = Disable (default). ▪ **[1]** = Enable. (Applicable to FXO interfaces): ▪ SITDetectorEnable = 1 ▪ UserDefinedToneDetectorEnable = 1 ▪ DisconnectOnBusyTone = 1 (applicable for Busy, Reorder and SIT tones) **Note:** For this parameter to take effect, a device reset is required.
EMS: UDT Detector Frequency Deviation **[UDTDetectorFrequencyDeviation]**	Defines the deviation (in Hz) allowed for the detection of each signal frequency. The valid range is 1 to 50. The default value is 50. **Note:** For this parameter to take effect, a device reset is required.
EMS: CPT Detector Frequency Deviation **[CPTDetectorFrequencyDeviation]**	Defines the deviation (in Hz) allowed for the detection of each CPT signal frequency. The valid range is 1 to 30. The default value is 10. **Note:** For this parameter to take effect, a device reset is required.

10.12.7.3 Metering Tone Parameters

The metering tone parameters are described in the table below.

Table 10-55: Metering Tone Parameters

Parameter	Description
Web: Generate Metering Tones EMS: Metering Mode **[PayPhoneMeteringMode]**	Determines the method used to configure the metering tones that are generated to the Tel side. ▪ **[0]** Disable = Metering tones aren't generated (default). ▪ **[1]** Internal Table = Metering tones are generated according to the internal table configured by the parameter ChargeCode. **Notes:** ▪ This parameter is applicable only to FXS interfaces. ▪ If you select 'Internal Table', you must configure the 'Charge Codes Table' (see "Configuring Charge Codes Table" on page 151).
Web: Analog Metering Type EMS: Metering Type **[MeteringType]**	Determines the metering method for generating pulses (sinusoidal metering burst frequency) by the FXS port. ▪ **[0]** 12 KHz (default) = 12 kHz sinusoidal bursts ▪ **[1]** 16 KHz = 16 kHz sinusoidal bursts ▪ **[2]** = Polarity Reversal pulses **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is applicable only to FXS interfaces.

Parameter	Description
Web: Analog TTX Voltage Level EMS: TTX Voltage Level **[AnalogTTXVoltageLevel]**	Determines the metering signal/pulse voltage level (TTX). ▪ **[0]** 0V = 0 Vrms sinusoidal bursts ▪ **[1]** 0.5V = 0.5 Vrms sinusoidal bursts (default) ▪ **[2]** 1V = 1 Vrms sinusoidal bursts **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is applicable only to FXS interfaces.
Web: Charge Codes Table **EMS: Charge Codes**	
[ChargeCode]	This *ini* file table parameter configures metering tones (and their time intervals) that the device's FXS interface generates to the Tel side. The format of this parameter is as follows: [ChargeCode] 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; [\ChargeCode] Where, ▪ EndTime = Period (1 - 4) end time. ▪ PulseInterval = Period (1 - 4) pulse interval. ▪ PulsesOnAnswer = Period (1 - 4) pulses on answer. 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; **Notes:** ▪ The parameter can include up to 25 indices (i.e., up to 25 different metering rules can be defined). ▪ This parameter is applicable only to FXS interfaces. ▪ To associate a charge code to an outgoing Tel-to-IP call, use the 'Tel to IP Routing'. ▪ To configure the Charge Codes table using the Web interface, see "Configuring Charge Codes Table" on page 151. ▪ For an explanation on configuration using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.12.8 Telephone Keypad Sequence Parameters

The telephony keypad sequence parameters are described in the table below.

Table 10-56: Keypad Sequence Parameters

Parameter	Description
Web/EMS: Call Pickup Key **[KeyCallPickup]**	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. The valid value is a string of up to 15 characters (0-9, #, and *). The default is undefined. **Notes:** ▪ Call pick-up is configured only for FXS endpoints pertaining to the same Hunt Group. ▪ This parameter is applicable only to FXS interfaces.
Prefix for External Line	
[Prefix2ExtLine]	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. The valid range is a one-character string. The default is an empty string. **Notes:** ▪ You can enable the device to add this string as the prefix to the collected (and sent) digits, using the parameter AddPrefix2ExtLine. ▪ This parameter is applicable only to FXS interfaces.
[AddPrefix2ExtLine]	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). ▪ **[0]** = Disable (default) ▪ **[1]** = Enable For example, if this parameter is enabled and the prefix string for 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. **Note:** This parameter is applicable only to FXS interfaces.

Parameter	Description
Hook Flash Parameters	
Web: Flash Keys Sequence Style **[FlashKeysSequenceStyle]**	Hook flash keys sequence style for FXS interfaces. ▪ **[0]** 0 = Flash hook (default) - only the phone's Flash button is used, according to the following scenarios: ✓ 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. ✓ 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. ▪ **[1]** 1 = Sequence of Flash hook and digit: ✓ Flash + 1: holds a call or toggles between two existing calls ✓ Flash + 2: makes a call transfer. ✓ 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). ▪ **[2]** 2 = Sequence of Flash Hook and digit: ✓ Flash Hook only: places a call on hold. ✓ Flash + 2: places a call on hold and answers a call-waiting call, or toggles between active and on-hold calls. ✓ Flash + 3: makes a three-way conference call (if the Enable3WayConference parameter is set to 1 and the 3WayConferenceMode parameter is set to 2). Note that the settings of the ConferenceCode parameter are ignored. ✓ Flash + 4: makes a call transfer.
Web: Flash Keys Sequence Timeout **[FlashKeysSequenceTimeout]**	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). The valid range is 100 to 5,000. The default is 2,000.
Keypad Feature - Call Forward Parameters	
Web: Unconditional EMS: Call Forward Unconditional **[KeyCFUnCond]**	Keypad sequence that activates the immediate call forward option.
Web: No Answer EMS: Call Forward No Answer **[KeyCFNoAnswer]**	Keypad sequence that activates the forward on no answer option.
Web: On Busy EMS: Call Forward Busy **[KeyCFBusy]**	Keypad sequence that activates the forward on busy option.
Web: On Busy or No Answer EMS: CF Busy Or No Answer **[KeyCFBusyOrNoAnswer]**	Keypad sequence that activates the forward on 'busy or no answer' option.

Parameter	Description
Web: Do Not Disturb EMS: CF Do Not Disturb **[KeyCFDoNotDisturb]**	Keypad sequence that activates the Do Not Disturb option (immediately reject incoming calls).
To activate the required forward method from the telephone: 1 Dial the user-defined sequence number on the keypad; a dial tone is heard. 2 Dial the telephone number to which the call is forwarded (terminate the number with #); a confirmation tone is heard.	
Web: Deactivate EMS: Call Forward Deactivation **[KeyCFDeact]**	Keypad sequence that deactivates any of the call forward options. After the sequence is pressed, a confirmation tone is heard.
Keypad Feature - Caller ID Restriction Parameters	
Web: Activate EMS: CLIR **[KeyCLIR]**	Keypad sequence that activates the restricted Caller ID option. After the sequence is pressed, a confirmation tone is heard.
Web: Deactivate EMS: CLIR Deactivation **[KeyCLIRDeact]**	Keypad sequence that deactivates the restricted Caller ID option. After the sequence is pressed, a confirmation tone is heard.
Keypad Feature - Hotline Parameters	
Web: Activate EMS: Hot Line **[KeyHotLine]**	Keypad sequence that activates the delayed hotline option. To activate the delayed hotline option from the telephone, perform the following: 1 Dial the user-defined sequence number on the keypad; a dial tone is heard. 2 Dial the telephone number to which the phone automatically dials after a configurable delay (terminate the number with #); a confirmation tone is heard.
Web: Deactivate EMS: Hot Line Deactivation **[KeyHotLineDeact]**	Keypad sequence that deactivates the delayed hotline option. After the sequence is pressed, a confirmation tone is heard.
Keypad Feature - Transfer Parameters	
Web: Blind EMS: Blind Transfer **[KeyBlindTransfer]**	Keypad sequence that activates blind transfer for Tel-to-IP calls. There are two possible scenarios: ▪ Option 1: After this sequence is dialed, the current call is put on hold (using Re-INVITE), a dial tone is played to the phone and then phone number collection starts. ▪ Option 2: A Hook-Flash is pressed, the current call is put on hold, a dial tone is played to the phone, and then digit collection starts. After this sequence is identified, the device continues the collection of the destination phone number. For both options, after the phone number is collected, it's sent to the transferee in a SIP REFER request (without a Replaces header). The call is then terminated and a confirmation tone is played to the phone. If the phone number collection fails due to a mismatch, a reorder tone is played to the phone. **Notes:** ▪ This parameter is applicable to FXO and FXS interfaces (but for FXO the Web interface does not display this parameter). ▪ It is possible to configure whether the KeyBlindTransfer code

Parameter	Description
	is added as a prefix to the dialed destination number, by using the parameter KeyBlindTransferAddPrefix.
Keypad Feature - Call Waiting Parameters	
Web: Activate EMS: Keypad Features CW **[KeyCallWaiting]**	Keypad sequence that activates the Call Waiting option. After the sequence is pressed, a confirmation tone is heard.
Web: Deactivate EMS: Keypad Features CW Deact **[KeyCallWaitingDeact]**	Keypad sequence that deactivates the Call Waiting option. After the sequence is pressed, a confirmation tone is heard.
Keypad Feature - Reject Anonymous Call Parameters	
Web: Activate EMS: Reject Anonymous Call **[KeyRejectAnonymousCall]**	Keypad sequence that activates the reject anonymous call option, whereby the device rejects incoming anonymous calls. After the sequence is pressed, a confirmation tone is heard.
Web: Deactivate EMS: Reject Anonymous Call Deact **[KeyRejectAnonymousCallDeact]**	Keypad sequence that de-activates the reject anonymous call option. After the sequence is pressed, a confirmation tone is heard.
[RejectAnonymousCallPerPort]	This *ini* file table parameter determines whether the device rejects incoming anonymous calls on FXS interfaces. The format of this parameter is as follows: [RejectAnonymousCallPerPort] FORMAT RejectAnonymousCallPerPort_Index = RejectAnonymousCallPerPort_Enable; [\RejectAnonymousCallPerPort] Where, ▪ Enable = accept **[0]** (default) or reject **[1]** incoming anonymous calls. For example: RejectAnonymousCallPerPort 0 = 0; RejectAnonymousCallPerPort 1 = 1; If enabled, when a device's FXS interface receives an anonymous call, it responds with a 433 (Anonymity Disallowed) SIP response. **Notes:** ▪ This parameter is applicable only to FXS interfaces. ▪ This parameter is per device. ▪ This parameter can appear up to 8 times for 8-port MP-11x devices and up to 24 times for MP-124 devices. ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.12.9 General FXO Parameters

The general FXO parameters are described in the table below.

Table 10-57: General FXO Parameters

Parameter	Description
Web: FXO Coefficient Type EMS: Country Coefficients **[CountryCoefficients]**	Determines the FXO line characteristics (AC and DC) according to USA or TBR21 standard. ▪ **[66]** Europe = TBR21 ▪ **[70]** USA = United States (default) **Note:** For this parameter to take effect, a device reset is required.
[FXONumberOfRings]	Defines the number of rings before the device's FXO interface answers a call by seizing the line. The valid range is 0 to 10. The default is 0. When set to 0, the FXO seizes the line after one ring. When set to 1, the FXO seizes the line after two rings. **Notes:** ▪ This parameter is applicable only if automatic dialing is not used. ▪ 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.
Web/EMS: Dialing Mode **[IsTwoStageDial]**	Determines the dialing mode for IP-to-Tel (FXO) calls. ▪ **[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. ▪ **[1]** Two Stages = Two-stage dialing (default). 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. **Notes:** ▪ This parameter is applicable only to FXO interfaces. ▪ This parameter can also be configured per Tel Profile, using the TelProfile parameter.
Web/EMS: Waiting For Dial Tone **[IsWaitForDialTone]**	Determines whether the device waits for a dial tone before dialing the phone number for IP-to-Tel (FXO) calls. ▪ **[0]** No = Don't wait for dial tone. ▪ **[1]** Yes = Wait for dial tone (default). When one-stage dialing and this parameter are enabled, the device dials the phone number (to the PSTN/PBX line) only 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. **Notes:** ▪ The correct dial tone parameters must be configured in the CPT file. ▪ The device may take 1 to 3 seconds to detect a dial tone (according

Parameter	Description
	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. ▪ This parameter is applicable only to FXO interfaces.
Web: Time to Wait before Dialing **[msec]** EMS: Time Before Dial **[WaitForDialTime]**	Determines the delay before the device starts dialing on the FXO line in the following scenarios: ▪ The delay between the time the line is seized and dialing begins during the establishment of an IP-to-Tel call. **Note:** Applicable only for one-stage dialing when the parameter IsWaitForDialTone is disabled. ▪ 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). ▪ For call transfer - the delay after hook-flash is generated and dialing begins. The valid range (in milliseconds) is 0 to 20,000 (i.e., 20 seconds). The default value is 1,000 (i.e., 1 second). **Note:** This parameter is applicable only to FXO interfaces.
Web: Ring Detection Timeout **[sec]** EMS: Timeout Between Rings **[FXOBetweenRingTime]**	Defines the timeout (in seconds) for detecting the second ring after the first detected ring. 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. 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. This parameter is typically set to between 5 and 8. The default is 8. **Notes:** ▪ This parameter is applicable only to FXO interfaces (for Tel-to-IP calls). ▪ 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).

Parameter	Description
Web: Rings before Detecting Caller ID EMS: Rings Before Caller ID **[RingsBeforeCallerID]**	Determines the number of rings before the device starts detecting Caller ID. ▪ **[0]** 0 = Before first ring. ▪ **[1]** 1 = After first ring (default). ▪ **[2]** 2 = After second ring. **Note:** This parameter is applicable only to FXO interfaces.
Web/EMS: Guard Time Between Calls **[GuardTimeBetweenCalls]**	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 value is 1. **Notes:** ▪ 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. ▪ This parameter is applicable only to FXO interfaces.

10.12.10 FXS Parameters

The general FXS parameters are described in the table below.

Table 10-58: General FXS Parameters

Parameter	Description
Web: FXS Coefficient Type EMS: Country Coefficients **[FXSCountryCoefficients]**	Determines the FXS line characteristics (AC and DC) according to USA or Europe (TBR21) standards. ▪ **[66]** Europe = TBR21 ▪ **[70]** USA = United States (default) **Note:** For this parameter to take effect, a device reset is required.

10.12.11 Hunt Groups, Number Manipulation and Routing Parameters

This subsection describes the device's number manipulation and routing parameters.

10.12.11.1 Hunt Groups and Routing Parameters

The routing parameters are described in the table below.

Table 10-59: Routing Parameters

Parameter	Description
Web: Endpoint Phone Number Table **EMS: SIP Endpoints > Phones**	
[TrunkGroup]	This *ini* file table parameter is used to define and activate the device's endpoints, by defining telephone numbers and assigning them to Hunt Groups. The format of this parameter is shown below: [TrunkGroup] FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum, TrunkGroup_FirstTrunkId, TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel, TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId, TrunkGroup_LastTrunkId, TrunkGroup_Module; [\TrunkGroup] For example, the configuration below assigns channels 1 through 4 to Hunt Group 1 and assigns phone numbers 101 to Channel 1, 102 to Channel 2, and so on: TrunkGroup 0 = 1, 255, 1, 4, 101, 0, 255, 255; **Notes:** ▪ The first entry in this table starts at index 0. ▪ Each endpoint (i.e., channel) must be assigned a unique phone number. In other words, no two endpoints can have the same phone number. ▪ The parameters TrunkGroup_FirstTrunkId, TrunkGroup_LastTrunkId, and TrunkGroup_Module are not applicable. ▪ For configuring this table in the Web interface, see Configuring Endpoint Phone Numbers on page 124 . ▪ For a description of *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
Web: Hunt Group Settings **EMS: SIP Routing > Hunt Group**	
[TrunkGroupSettings]	This *ini* file table parameter defines rules for channel allocation per Hunt Group. If no rule exists, the rule defined by the global parameter ChannelSelectMode takes effect. The format of this parameter is as follows: [TrunkGroupSettings] FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId, TrunkGroupSettings_ChannelSelectMode, TrunkGroupSettings_RegistrationMode, TrunkGroupSettings_GatewayName,TrunkGroupSettings_ContactUser, TrunkGroupSettings_ServingIPGroup,

Parameter	Description
	TrunkGroupSettings_MWIInterrogationType; [\TrunkGroupSettings] For example: TrunkGroupSettings 0 = 1, 0, 5, branch-hq, user, 1, 255; TrunkGroupSettings 1 = 2, 1, 0, localname, user1, 2, 255; **Notes:** ▪ This parameter can include up to 24 indices. ▪ The parameter MWIInterrogationType is not applicable. ▪ For configuring Hunt Group Settings using the Web interface, see "Configuring Hunt Group Settings" on page 126. ▪ For a description on using *ini* file table parameters, see to "Configuring ini File Table Parameters" on page 194.
Web: Channel Select Mode EMS: Channel Selection Mode **[ChannelSelectMode]**	Method for allocating incoming IP-to-Tel calls to a channel (port). ▪ **[0]** By Dest Phone Number = Selects the device's channel according to the called number (default.) ▪ **[1]** Cyclic Ascending = Selects the next available channel in an ascending cyclic order. Always selects the next higher channel number in the Hunt Group. When the device reaches the highest channel number in the Hunt Group, it selects the lowest channel number in the Hunt Group and then starts ascending again. ▪ **[2]** Ascending = Selects the lowest available channel. It always starts at the lowest channel number in the Hunt Group and if that channel is unavailable, selects the next higher channel. ▪ **[3]** Cyclic Descending = Selects the next available channel in descending cyclic order. It always selects the next lower channel number in the Hunt Group. When the device reaches the lowest channel number in the Hunt Group, it selects the highest channel number in the Hunt Group and then starts descending again. ▪ **[4]** Descending = Selects the highest available channel. It always starts at the highest channel number in the Hunt Group and if that channel is unavailable, selects the next lower channel. ▪ **[5]** Dest Number + Cyclic Ascending = The device first selects the channel according to the called number. If the called number isn't found, it then selects the next available channel in ascending cyclic order. Note that if the called number is found but the port associated with this number is busy, the call is released. ▪ **[6]** By Source Phone Number = The device selects the channel according to the calling number. ▪ **[9]** Ring to Hunt Group = The device allocates IP-to-Tel calls to all the FXS ports (channels) pertaining to a specific Hunt Group. When an IP-to-Tel call is received by the device for a specific Hunt Group, all telephones connected to the FXS ports belonging to the Hunt Group start ringing. The call is eventually received by whichever telephone answers the call first (and the other phones then stop ringing). This option is applicable only to FXS interfaces.

Parameter	Description
	Notes: ▪ For defining the channel select mode per Hunt Group, see "Configuring Hunt Group Settings" on page 126. ▪ The phone numbers of the device's channels are defined by the TrunkGroup parameter.
Web: Default Destination Number **[DefaultNumber]**	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 'Endpoint Phone Number Table' (see to Configuring Endpoint Phone Numbers on page 124). This parameter is used as a starting number for the list of channels comprising all the device's Hunt Groups. The default value is 1000.
Web: Source IP Address Input **[SourceIPAddressInput]**	Determines the IP address that the device uses to determine the source of incoming INVITE messages for IP-to-Tel routing. ▪ **[-1]** = Not configured. (default) ▪ **[0]** SIP Contact Header = The IP address in the Contact header of the incoming INVITE message is used. ▪ **[1]** Layer 3 Source IP = The actual IP address (Layer 3) from where the SIP packet was received is used.
Web: Use Source Number As Display Name EMS: Display Name **[UseSourceNumberAsDisplayName]**	Determines the use of Tel Source Number and Display Name for Tel-to-IP calls. ▪ **[0]** No = 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 (default). ▪ **[1]** 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. ▪ **[2]** 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).
Web/EMS: Use Display Name as Source Number **[UseDisplayNameAsSourceNumber]**	Determines the use of Source Number and Display Name for IP-to-Tel calls. ▪ **[0]** No = 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 (default). ▪ **[1]** 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). For example: When 'From: 100 <sip:200@201.202.203.204>' is received, the outgoing Source Number and Display Name are set to '100' and the Presentation is set to Allowed (0). When 'From: <sip:100@101.102.103.104>' is received, the outgoing Source Number is set to '100' and the Presentation is set to Restricted (1).

Parameter	Description
Web: Use Routing Table for Host Names and Profiles EMS: Use Routing Table For Host Names **[AlwaysUseRouteTable]**	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. ▪ **[0]** Disable = Don't use internal routing table (default). ▪ **[1]** Enable = Use the 'Tel to IP Routing'. **Notes:** ▪ This parameter appears only if the 'Use Default Proxy' parameter is enabled. ▪ The domain name is used instead of a Proxy name or IP address in the INVITE SIP URI.
Web/EMS: Tel to IP Routing Mode **[RouteModeTel2IP]**	For a description of this parameter, see "Configuring Tel to IP Routing" on page 138.
Web: Tel to IP Routing **EMS: SIP Routing > Tel to IP**	
[Prefix]	This *ini* file table parameter configures the 'Tel to IP Routing' for routing Tel-to-IP calls. The format of this parameter is as follows: [PREFIX] 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] 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; **Notes:** ▪ This parameter can include up to 50 indices. ▪ The following parameters are not applicable: PREFIX_SrcIPGroupID, PREFIX_DestHostPrefix, PREFIX_SrcHostPrefix, PREFIX_DestSRD. ▪ For a detailed description of the table's parameters and for configuring this table using the Web interface, see "Configuring Tel to IP Routing" on page 138. ▪ For a description on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

Parameter	Description
Web: IP to Hunt Group Routing Table **EMS: SIP Routing > IP to Hunt**	
[PSTNPrefix]	This *ini* file table parameter configures the routing of IP calls to Hunt Groups. The format of this parameter is as follows: [PSTNPrefix] FORMAT PstnPrefix_Index = PstnPrefix_DestPrefix, PstnPrefix_TrunkGroupId, PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress, PstnPrefix_ProfileId, PstnPrefix_SrcIPGroupID, PstnPrefix_DestHostPrefix, PstnPrefix_SrcHostPrefix; [\PSTNPrefix] For example: PstnPrefix 0 = 100, 1, 200, *, 0, 2, , ; PstnPrefix 1 = *, 2, *, , 1, 3, acl, joe; **Notes:** ▪ This parameter can include up to 24 indices. ▪ For a description of the table's parameters, refer to the corresponding Web parameters in "Configuring IP to Hunt Group Routing Table" on page 142. ▪ To support the In-Call Alternative Routing feature, you can use two entries that support the same call but assigned with a different Hunt Group. The second entry functions as an alternative route if the first rule fails as a result of one of the release reasons configured in the AltRouteCauseIP2Tel table. ▪ Selection of Hunt Groups (for IP-to-Tel calls) is according to destination number, source number,and source IP address. ▪ The source IP address (SourceAddress) can include the 'x' wildcard to represent single digits. For example: 10.8.8.xx represents all IP addresses between 10.8.8.10 and 10.8.8.99. ▪ The source IP address (SourceAddress) 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. ▪ If the source IP address (SourceAddress) includes an FQDN, DNS resolution is performed according to the parameter DNSQueryType. ▪ For available notations for depicting a range of multiple numbers, see "Dialing Plan Notation for Routing and Manipulation" on page 228. ▪ For a description on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
Web/EMS: IP to Tel Routing Mode **[RouteModeIP2Tel]**	Determines whether to route IP calls to the Hunt Group before or after manipulation of the destination number (configured in "Configuring Number Manipulation Tables" on page 129). ▪ **[0]** Route calls before manipulation = Calls are routed before the number manipulation rules are applied (default). ▪ **[1]** Route calls after manipulation = Calls are routed after the number manipulation rules are applied.

Parameter	Description
Web: IP Security EMS: Secure Call From IP **[SecureCallsFromIP]**	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. ▪ **[0]** Disable = The device accepts all SIP calls (default). ▪ **[1]** Secure Incoming calls = The device accepts SIP calls (i.e., calls from the IP side) only from IP addresses that are defined in the 'Tel to IP Routing' 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. ▪ **[2]** Secure All calls = The device accepts SIP calls only from IP addresses (in dotted-decimal notation format) that are defined in the 'Tel to IP Routing' 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 **[1]** is that this option is concerned only about numerical IP addresses that are defined in the tables. **Note:** If this parameter is set to **[1]** or **[2],** 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.
Web/EMS: Filter Calls to IP **[FilterCalls2IP]**	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 115). ▪ **[0]** Don't Filter = device doesn't filter calls when using a Proxy (default). ▪ **[1]** Filter = Filtering is enabled. When this parameter is enabled and a Proxy is used, the device first checks the 'Tel to IP Routing'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. **Note:** When no Proxy is used, this parameter must be disabled and filtering is according to the 'Tel to IP Routing'.
Web: Add CIC **[AddCicAsPrefix]**	Determines whether to add the Carrier Identification Code (CIC) as a prefix to the destination phone number for IP-to-Tel calls. ▪ **[0]** No (default) ▪ **[1]** Yes 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 Hunt Group based on this parameter's value. 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

Parameter	Description
	Note: After the cic prefix is added, the 'IP to Hunt Group Routing Table' can be used to route this call to a specific Hunt Group. The Destination Number IP to Tel Manipulation table must be used to remove this prefix before placing the call to the Tel.

10.12.11.2 Alternative Routing Parameters

The alternative routing parameters are described in the table below.

Table 10-60: Alternative Routing Parameters

Parameter	Description
Web/EMS: Redundant Routing Mode **[RedundantRoutingMode]**	Determines the type of redundant routing mechanism when a call can't be completed using the main route. ▪ **[0]** 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. ▪ **[1]** Routing Table = Internal routing table is used to locate a redundant route (default). ▪ **[2]** Proxy = Proxy list is used to locate a redundant route. **Note:** To implement the Redundant Routing Mode mechansim, you first need to configure the parameter AltRouteCauseTEL2IP (Reasons for Alternative Routing table).
Web: Enable Alt Routing Tel to IP EMS: Enable Alternative Routing **[AltRoutingTel2IPEnable]**	Enables the Alternative Routing feature for Tel-to-IP calls. ▪ **[0]** Disable = Disables the Alternative Routing feature (default). ▪ **[1]** Enable = Enables the Alternative Routing feature. ▪ **[2]** Status Only = The Alternative Routing feature is disabled, but read-only information on the QoS of the destination IP addresses is provided. For information on the Alternative Routing feature, see "Configuring Alternative Routing (Based on Connectivity and QoS)" on page 247.
Web: Alt Routing Tel to IP Mode EMS: Alternative Routing Mode **[AltRoutingTel2IPMode]**	Determines the event(s) reason for triggering Alternative Routing. ▪ **[0]** None = Alternative routing is not used. ▪ **[1]** Connectivity = Alternative routing is performed if a ping or SIP OPTIONS message to the initial destination fails (determined according to the AltRoutingTel2IPConnMethod parameter). ▪ **[2]** QoS = Alternative routing is performed if poor QoS is detected. ▪ **[3]** Both = Alternative routing is performed if either ping to initial destination fails, poor QoS is detected, or the DNS host name is not resolved (default). **Notes:** ▪ 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. For information on the Alternative Routing feature, see

Parameter	Description
	"Configuring Alternative Routing (Based on Connectivity and QoS)" on page 247. ▪ To receive quality information (displayed in the 'Quality Status' and 'Quality Info.' fields in "Viewing IP Connectivity" on page 190) per destination, this parameter must be set to 2 or 3.
Web: Alt Routing Tel to IP Connectivity Method EMS: Alternative Routing Telephone to IP Connection Method **[AltRoutingTel2IPConnMethod]**	Determines the method used by the device for periodically querying the connectivity status of a destination IP address. ▪ **[0]** ICMP Ping (default) = Internet Control Message Protocol (ICMP) ping messages. ▪ **[1]** SIP OPTIONS = The remote destination is considered offline if the latest OPTIONS transaction timed out. Any response to an OPTIONS request, even if indicating an error, brings the connectivity status to online.
[EnableAltMapTel2IP]	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). ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
Web: Alt Routing Tel to IP Keep Alive Time EMS: Alternative Routing Keep Alive Time **[AltRoutingTel2IPKeepAliveTime]**	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 value is 60.
Web/EMS: Alternative Routing Tone Duration **[ms]** **[AltRoutingToneDuration]**	Determines the duration (in milliseconds) for which the device plays a tone to the endpoint on each Alternative Routing attempt. When the device finishes playing the tone, a new SIP INVITE message is sent to the new destination. The tone played is the Call Forward Tone (Tone Type #25 in the CPT file). The valid range is 0 to 20,000. The default is 0 (i.e., no tone is played).
Web: Max Allowed Packet Loss for Alt Routing **[%]** **[IPConnQoSMaxAllowedPL]**	Packet loss in percentage at which the IP connection is considered a failure and Alternative Routing mechanism is activated. The default value is 20%.
Web: Max Allowed Delay for Alt Routing **[msec]** **[IPConnQoSMaxAllowedDelay]**	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 value is 250.

Parameter	Description
Web: Reasons for Alternative Tel-to-IP Routing Table **EMS: Alt Route Cause Tel to IP**	
[AltRouteCauseTel2IP]	This *ini* file 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 (address) for the call in the 'Tel to IP Routing' (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. The format of this parameter is as follows: [AltRouteCauseTel2IP] FORMAT AltRouteCauseTel2IP_Index = AltRouteCauseTel2IP_ReleaseCause; [\AltRouteCauseTel2IP] For example: AltRouteCauseTel2IP 0 = 486; (Busy Here) AltRouteCauseTel2IP 1 = 480; (Temporarily Unavailable) AltRouteCauseTel2IP 2 = 408; (No Response) **Notes:** ▪ This parameter can include up to 5 indices. ▪ The reasons for alternative routing for Tel-to-IP calls apply only when a Proxy is not used. ▪ When there is no response to an INVITE message (after INVITE retransmissions), the device issues an internal 408 'No Response' implicit release reason. ▪ The device sends the call to an alternative IP route only after the call has failed and the device has subsequently attempted twice to establish the call unsuccessfully. ▪ 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 parameter AltRoutingToneDuration). ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194
Web: Reasons for Alternative IP-to-Tel Routing Table **EMS: Alt Route Cause IP to Tel**	
[AltRouteCauseIP2Tel]	This *ini* file table parameter configures call failure reason values received from the Tel side . If a call is released as a result of one of these reasons, the device attempts to locate an alternative Hunt Group for the call in the 'IP to Hunt Group Routing Table'. The format of this parameter is as follows: [AltRouteCauseIP2Tel] FORMAT AltRouteCauseIP2Tel_Index = AltRouteCauseIP2Tel_ReleaseCause; [\AltRouteCauseIP2Tel] For example: AltRouteCauseIP2Tel 0 = 3 (No Route to Destination) AltRouteCauseIP2Tel 1 = 1 (Unallocated Number) AltRouteCauseIP2Tel 2 = 17 (Busy Here) **Notes:**

Parameter	Description
	▪ This parameter can include up to 5 indices. ▪ This table can be used for example, in scenarios where the destination is busy and the Release Reason #17 is issued or for other call releases that issue the default Release Reason (#3). ▪ 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 parameter AltRoutingToneDuration). ▪ For an explanation on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
Web/EMS: Forward On Busy Trunk Destination	
[ForwardOnBusyTrunkDest]	This ini file table parameter configures the Forward On Busy Trunk Destination table. This table allows you to define an alternative IP destination - IP address or SIP Request-URI user name and host part (i.e., user@host) per Hunt Group for IP-to Tel calls. The IP-to-Tel call is forwarded to this IP destination (using 3xx response) if the following exists: The format of this parameter is as follows: [ForwardOnBusyTrunkDest] FORMAT ForwardOnBusyTrunkDest_Index = ForwardOnBusyTrunkDest_TrunkGroupId, ForwardOnBusyTrunkDest_ForwardDestination; [\ForwardOnBusyTrunkDest] 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. **Notes:** ▪ The maximum number of indices (starting from 1) depends on the maximum number of Hunt Groups. ▪ For the destination, instead of a dotted-decimal IP address, FQDN can be used. In addition, the following syntax can be used: "host:port;transport=xxx"(i.e., IP address, port and transport type). ▪ For a detailed description of this feature, see Configuring Call Forward upon Busy Trunk on page 146

10.12.11.3 Number Manipulation Parameters

The number manipulation parameters are described in the table below.

Table 10-61: Number Manipulation Parameters

Parameter	Description
Web: Copy Destination Number to Redirect Number EMS: Copy Dest to Redirect Number **[CopyDest2RedirectNumber]**	Determines whether the device copies the called number to the outgoing SIP Diversion header for Tel-to-IP calls. 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. ▪ **[0]** Don't copy = Disable (default). ▪ **[1]** 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. ▪ **[2]** 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. **Note:** This parameter can also be configured per IP Profile (using the IPProfile parameter).
Web/EMS: Add Hunt Group ID as Prefix **[AddTrunkGroupAsPrefix]**	Determines whether the Hunt Group ID is added as a prefix to the destination phone number (i.e., called number) for Tel-to-IP calls. ▪ **[0]** No = Don't add Hunt Group ID as prefix (default). ▪ **[1]** Yes = Add Hunt Group ID as prefix to called number. **Notes:** ▪ This option can be used to define various routing rules. ▪ To use this feature, you must configure the Hunt Group IDs (see Configuring Endpoint Phone Numbers on page 124).

Parameter	Description
Web: Add Trunk ID as Prefix EMS: Add Port ID As Prefix **[AddPortAsPrefix]**	Determines whether the port number is added as a prefix to the called number for Tel-to-IP calls. ▪ **[0]** No = port number not added as prefix (default). ▪ **[1]** Yes = port number added as prefix If enabled, the port number (single digit in the range 1 to 8for 8-port devices, two digits in the range 01 to 24 for MP-124) is added as a prefix to the called (destination) phone number. This option can be used to define various routing rules.
Web/EMS: Add Trunk Group ID as Prefix to Source **[AddTrunkGroupAsPrefixToSource]**	Determines whether the device adds the Hunt Group ID (from where the call originated) as the prefix to the calling number (i.e. source number). ▪ **[0]** No (default) ▪ **[1]** Yes
Web: IP to Tel Remove Routing Table Prefix EMS: Remove Prefix **[RemovePrefix]**	Determines whether the device removes the prefix from the destination number for IP-to-Tel calls. ▪ **[0]** No = Don't remove prefix (default) ▪ **[1]** Yes = Remove the prefix (defined in the 'IP to Hunt Group Routing Table' - see "Configuring IP to Hunt Group Routing Table" on page 142) from a telephone number for an IP-to-Tel call before forwarding it to Tel. For example: To route an incoming IP-to-Tel call with destination number 21100, the 'IP to Hunt Group 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 Hunt Group, the prefix (21) is removed from the original number, and therefore, only 100 remains. **Notes:** ▪ This parameter is applicable only if number manipulation is performed after call routing for IP-to-Tel calls (i.e., RouteModeIP2Tel parameter is set to 0). ▪ Similar operation (of removing the prefix) is also achieved by using the usual number manipulation rules.
[SwapTel2IPCalled&CallingNumbers]	If enabled, 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. ▪ **[0]** = Disabled (default) ▪ **[1]** = Swap calling and called numbers **Note:** This parameter can also be configure per Tel Profile, using the TelProfile parameter.

Parameter	Description
Web: Add Number Plan and Type to RPI Header EMS: Add Ton 2 RPI **[AddTON2RPI]**	Determines whether the TON/PLAN parameters are included in the Remote-Party-ID (RPID) header. ▪ **[0]** No ▪ **[1]** Yes (default) 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.
Web/EMS: Source Manipulation Mode **[SourceManipulationMode]**	Determines the SIP headers containing the source number after manipulation: ▪ **[0]** = The SIP From and P-Asserted-Identity headers contain the source number after manipulation (default). ▪ **[1]** = Only SIP From header contains the source number after manipulation, while the P-Asserted-Identity header contains the source number before manipulation.
Web: Redirect Number Tel -> IP **EMS: Redirect Number Map Tel to IP**	
[RedirectNumberMapTel2IP]	This ini file table parameter manipulates the redirect number for Tel-to-IP calls. The manipulated Redirect Number is sent in the SIP Diversion, History-Info, or Resource-Priority headers. The format of this parameter is as follows: [RedirectNumberMapTel2Ip] FORMAT RedirectNumberMapTel2Ip_Index = RedirectNumberMapTel2Ip_DestinationPrefix, RedirectNumberMapTel2Ip_RedirectPrefix, RedirectNumberMapTel2Ip_NumberType, RedirectNumberMapTel2Ip_NumberPlan, RedirectNumberMapTel2Ip_RemoveFromLeft, RedirectNumberMapTel2Ip_RemoveFromRight, RedirectNumberMapTel2Ip_LeaveFromRight, RedirectNumberMapTel2Ip_Prefix2Add, RedirectNumberMapTel2Ip_Suffix2Add, RedirectNumberMapTel2Ip_IsPresentationRestricted, RedirectNumberMapTel2Ip_SrcTrunkGroupID, RedirectNumberMapTel2Ip_SrcIPGroupID; [\RedirectNumberMapTel2Ip] For example: RedirectNumberMapTel2Ip 1 = *, 4, 255, 255, 0, 0, 255, , 972, 255, 1, 2; **Notes:** ▪ This parameter table can include up to 20 indices (1-20). ▪ The manipulation rules are done in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and then Suffix2Add. ▪ If the table's matching characteristics rule (i.e., DestinationPrefix, RedirectPrefix, SrcTrunkGroupID, and SrcIPGroupID) is located for the Tel-to-IP call, then the redirect number manipulation rule (defined by

Parameter	Description
	the other parameters) is applied to the call. ▪ Redirect number manipulation for Tel-to-IP calls is not performed if the CopyDest2RedirectNumber parameter is enabled. This parameter copies the received destination number to the outgoing redirect number. ▪ The following parameters are not applicable: NumberType, NumberPlan, and IsPresentationRestricted.
Web: Destination Phone Number Manipulation Table for Tel to IP Calls **EMS: SIP Manipulations > Destination Telcom to IPs**	
[NumberMapTel2IP]	This *ini* file table parameter manipulates the destination number of Tel-to-IP calls. The format of this parameter is as follows: [NumberMapTel2Ip] 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_ SrcIPGroupID; [\NumberMapTel2Ip] For example: NumberMapTel2Ip 0 = 01,$$,*,0,0,2,$$,$$,971,$$,$$,$$,$$; NumberMapTel2Ip 1 = 10,10,*,255,255,3,0,5,100,$$,255,$$,$$; **Notes:** ▪ This table parameter can include up to 120 indices (0-119). ▪ The manipulation rules are done in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and then Suffix2Add. ▪ If the called and calling numbers match the DestinationPrefix and/or SourcePrefix conditions, then the parameters RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, and/or LeaveFromRight are applied. ▪ The following parameters are not applicable: SrcIPGroupID, NumberType, NumberPlan, SourceAddress and IsPresentationRestricted. ▪ To configure manipulation of destination numbers for Tel-to-IP calls using the Web interface, see "Configuring the Number Manipulation Tables" on page 129).

Parameter	Description
	▪ For a description on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
Web: Destination Phone Number Manipulation Table for IP to Tel Calls **EMS: EMS: SIP Manipulations > Destination IP to Telcom**	
[NumberMapIP2Tel]	This *ini* file table parameter manipulates the destination number of IP-to-Tel calls. The format of this parameter is as follows: [NumberMapIp2Tel] 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; [\NumberMapIp2Tel] For example: NumberMapIp2Tel 0 = 03,22,$$,$$,$$,2,667,$$,$$; **Notes:** ▪ This table parameter can include up to 100 indices. ▪ The manipulation rules are done in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and then Suffix2Add. ▪ If the called and calling numbers match the DestinationPrefix, SourcePrefix, and/or SourceAddress conditions, then the RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, and/or LeaveFromRight are applied. ▪ The Source IP address can include the following wildcards: ✓ 'x': represents single digits. For example: 10.8.8.xx represents addresses between 10.8.8.10 and 10.8.8.99. ✓ '*' (asterisk): represents any number between 0 and 255. For example, 10.8.8.* represents addresses between 10.8.8.0 and 10.8.8.255. ▪ The following parameters isare not applicable: SrcIPGroupID, NumberType, NumberPlan and IsPresentationRestricted. ▪ To configure manipulation of destination numbers for IP-to-Tel calls using the Web interface, see "Configuring Number Manipulation Tables" on page 129). ▪ For a description on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

Parameter	Description
[PerformAdditionalIP2TELDestination Manipulation]	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). ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
Web: Source Phone Number Manipulation Table for Tel to IP Calls **EMS: SIP Manipulations > Source Telcom to IP**	
[SourceNumberMapTel2IP]	This *ini* file table parameter manipulates the source phone number for Tel-to-IP calls. The format of this parameter is as follows: [SourceNumberMapTel2Ip] FORMAT SourceNumberMapTel2Ip_Index = SourceNumberMapTel2Ip_DestinationPrefix, SourceNumberMapTel2Ip_SourcePrefix, SourceNumberMapTel2Ip_SourceAddress, SourceNumberMapTel2Ip_NumberType, SourceNumberMapTel2Ip_NumberPlan, SourceNumberMapTel2Ip_RemoveFromLeft, SourceNumberMapTel2Ip_RemoveFromRight, SourceNumberMapTel2Ip_LeaveFromRight, SourceNumberMapTel2Ip_Prefix2Add, SourceNumberMapTel2Ip_Suffix2Add, SourceNumberMapTel2Ip_IsPresentationRestricted, NumberMapTel2Ip_SrcTrunkGroupID, NumberMapTel2Ip_SrcIPGroupID; [\SourceNumberMapTel2Ip] For example: SourceNumberMapTel2Ip 0 = 22,03,$$,0,0,$$,2,$$,667,$$,0,$$,$$; SourceNumberMapTel2Ip 0 = 10,10,*,255,255,3,0,5,100,$$,255,$$,$$; **Notes:** ▪ This table parameter can include up to 20 indices. ▪ The manipulation rules are done in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and then Suffix2Add. ▪ If the called and calling numbers match the DestinationPrefix and/or SourcePrefix conditions, then the RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, NumberPlan, and/or IsPresentationRestricted are applied. ▪ An asterisk ('*') represents all IP addresses. ▪ IsPresentationRestricted is set to 'Restricted' only if 'Asserted Identity Mode' is set to 'P-Asserted'. ▪ The following parameters are not applicable: NumberType and NumberPlan.

Parameter	Description
	▪ To configure manipulation of source numbers for Tel-to-IP calls using the Web interface, see "Configuring Number Manipulation Tables" on page 129). ▪ For a description on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.
Web: Source Phone Number Manipulation Table for IP to Tel Calls **EMS: EMS: SIP Manipulations > Source IP to Telcom**	
[SourceNumberMapIP2Tel]	This *ini* file table parameter manipulates the source number for IP-to-Tel calls. The format of this parameter is as follows: [SourceNumberMapIp2Tel] 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; [\SourceNumberMapIp2Tel] For example: SourceNumberMapIp2Tel 0 = 22,03,$$,$$,$$,$$,2,667,$$,$$; SourceNumberMapIp2Tel 1 = 034,01,1.1.1.1,$$,0,2,$$,$$,972,$$,10; **Notes:** ▪ This table parameter can include up to 20 indices. ▪ The manipulation rules are done in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and then Suffix2Add. ▪ If the called and calling numbers match the DestinationPrefix, SourcePrefix, and/or SourceAddress conditions, then the RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, and/or LeaveFromRight are applied. ✓ 'x': represents single digits. For example: 10.8.8.xx represents addresses between 10.8.8.10 and 10.8.8.99. ✓ '*' (asterisk): represents any number between 0 and 255. For example, 10.8.8.* represents addresses between 10.8.8.0 and 10.8.8.255. ▪ The following parameters are not applicable: NumberType, NumberPlan and IsPresentationRestricted. ▪ To configure manipulation of source numbers for IP-to-Tel calls using the Web interface, see "Configuring Number Manipulation Tables" on page 129). ▪ For a description on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page

Parameter	Description
	194.
[PerformAdditionalIP2TELSourceManipulation]	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). ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
Phone-Context Parameters	
Web/EMS: Add Phone Context As Prefix **[AddPhoneContextAsPrefix]**	Determines whether the received Phone-Context parameter is added as a prefix to the outgoing Called and Calling numbers. ▪ **[0]** Disable = Disable (default). ▪ **[1]** Enable = Enable.
Web: Phone Context Table **EMS: SIP Manipulations > Phone Context**	
[PhoneContext]	This *ini* file table parameter defines the Phone Context table. This parameter maps NPI and TON to the SIP Phone-Context parameter. When a call is received from the Tel, the NPI and TON are compared against the table and the corresponding Phone-Context value is used in the outgoing SIP INVITE message. The same mapping occurs when an INVITE with a Phone-Context attribute is received. The Phone-Context parameter appears in the standard SIP headers (Request-URI, To, From, Diversion) where a phone number is used. The format for this parameter is as follows: [PhoneContext] FORMAT PhoneContext_Index = PhoneContext_Npi, PhoneContext_Ton, PhoneContext_Context; [\PhoneContext] For example: PhoneContext 0 = 0,0,unknown.com PhoneContext 1 = 1,1,host.com PhoneContext 2 = 9,1,na.e164.host.com **Notes:** ▪ This parameter can include up to 20 indices. ▪ Several entries with the same NPI-TON or Phone-Context are allowed. In this scenario, a Tel-to-IP call uses the first match. ▪ To configure the Phone Context table using the Web interface, see "Mapping NPI/TON to SIP Phone-Context" on page 135. ▪ For a description on using *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.13 Standalone Survivability Parameters

The Stand-alone Survivability (SAS) parameters are described in the table below.

Table 10-62: SAS Parameters

Parameter	Description
Web: Enable SAS EMS: Enable **[EnableSAS]**	Enables the Stand-Alone Survivability (SAS) feature. ▪ **[0]** Disable Disabled (default) ▪ **[1]** Enable = SAS is enabled 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. **Note:** For this parameter to take effect, a device reset is required.
Web: SAS Local SIP UDP Port EMS: Local SIP UDP **[SASLocalSIPUDPPort]**	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. The valid range is 1 to 65,534. The default value is 5080.
Web: SAS Default Gateway IP EMS: Default Gateway IP **[SASDefaultGatewayIP]**	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. The address can be configured as an IP address (dotted-decimal notation) or as a domain name (up to 49 characters). The default is a null string, which is interpreted as the local IP address of the gateway.
Web: SAS Registration Time EMS: Registration Time **[SASRegistrationTime]**	Determines 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'. The valid range is 0 (Analog) to 2,000,000. The default value is 20.
Web: SAS Local SIP TCP Port EMS: Local SIP TCP Port **[SASLocalSIPTCPPort]**	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. The valid range is 1 to 65,534. The default value is 5080.
Web: SAS Local SIP TLS Port EMS: Local SIP TLS Port **[SASLocalSIPTLSPort]**	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. The valid range is 1 to 65,534. The default value is 5081.
Web/EMS: Enable Record-Route **[SASEnableRecordRoute]**	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. ▪ **[0]** Disable (default) ▪ **[1]** Enable 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

Parameter	Description
	header, causing all future dialogs in the session to pass through it as well. When this feature is enabled, the SIP Record-Route header includes the URI "lr" parameter. The presence of this parameter indicates loose routing; the lack of 'lt' indicates strict routing. For example: ▪ Loose routing: Record-Route: <sip:server10.biloxi.com;lr> ▪ Strict routing: Record-Route: <sip:bigbox3.site3.atlanta.com>
Web: SAS Proxy Set EMS: Proxy Set **[SASProxySet]**	Determines 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. The valid range is 0 to 5. The default value is 0 (i.e., default Proxy Set).
Web: Redundant SAS Proxy Set EMS: Redundant Proxy Set **[RedundantSASProxySet]**	Determines 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). The valid range is -1 to 5. The default value is -1 (i.e., no redundant Proxy Set).
Web/EMS: SAS Block Unregistered Users **[SASBlockUnRegUsers]**	Determines whether the device rejects SIP INVITE requests received from unregistered SAS users. This applies to SAS Normal and Emergency modes. ▪ **[0]** Un-Block = Allow INVITE from unregistered SAS users (default). ▪ **[1]** Block = Reject dialog-establishment requests from un-registered SAS users.
[SASEnableContactReplace]	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. ▪ **[0]** (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. ▪ **[1]** = 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. **Note:** Operating in this mode causes all incoming dialog requests to traverse the SAS, which may cause load problems.
Web: SAS Survivability Mode EMS: Survivability Mode **[SASSurvivabilityMode]**	Determines the Survivability mode used by the SAS application. ▪ **[0]** Standard = 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

Parameter	Description
	(default). ▪ **[1]** 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). ▪ **[2]** Ignore Register = Use regular SAS Normal/Emergency logic (same as option **[0]),** but when in Normal mode incoming REGISTER requests are ignored. ▪ **[3]** 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. ▪ **[4]** 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).
Web: Enable ENUM **[SASEnableENUM]**	Enables SAS to perform ENUM (E.164 number to URI mapping) queries when receiving INVITE messages in SAS emergency mode. ▪ **[0]** Disable (default) ▪ **[1]** Enable
Web: SAS Binding Mode EMS: Binding Mode **[SASBindingMode]**	Determines the SAS application database binding mode. ▪ **[0]** URI = 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 (default). ▪ **[1]** User Part only = The binding is always performed according to the User Part only.
Web: SAS Emergency Numbers **[SASEmergencyNumbers]**	Defines emergency numbers for the device's SAS application. When the device's SAS agent receives a SIP INVITE (from an IP phone) that includes one of the emergency numbers (in the SIP user part), it forwards the INVITE to the default gateway (configured by the parameter SASDefaultGatewayIP), i.e., the device itself, which sends the call directly to the PSTN. This is important for routing emergency numbers such as 911 (in North America) directly to the PSTN. This is applicable to SAS operating in Normal and Emergency modes. Up to four emergency numbers can be defined, where each number can be up to four digits.
[SASEmergencyPrefix]	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 'IP2IP 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 "".

Parameter	Description
Web: SAS Registration Manipulation Table EMS: Stand-Alone Survivability	
[SASRegistrationManipulation]	This *ini* file 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: [SASRegistrationManipulation] FORMAT SASRegistrationManipulation_Index = SASRegistrationManipulation_RemoveFromRight, SASRegistrationManipulation_LeaveFromRight; [\SASRegistrationManipulation] ▪ RemoveFromRight = number of digits removed from the right side of the user part before saving to the registered user database. ▪ LeaveFromRight = number of digits to keep from the right side. If both RemoveFromRight and LeaveFromRight are defined, the RemoveFromRight is applied first. The registered database contains the AoR before and after manipulation. The range of both RemoveFromRight and LeaveFromRight is 0 to 30. 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;` **Notes:** ▪ You can only configure one index entry. ▪ For a detailed description of the individual parameters in this table and for configuring this table using the Web interface, see "Configuring Stand-Alone Survivability" on page 161.
Web: SAS IP-to-IP Routing Table	
[IP2IPRouting]	This *ini* file table parameter configures the IP-to-IP Routing table for SAS routing rules. The format of this parameter is as follows: [IP2IPRouting] FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID, IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort, IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions; [\IP2IPRouting] For example: IP2IPRouting 1 = -1, *, *, *, *, 0, -1, -1, , 0, -1, 0; **Notes:** ▪ This table can include up to 120 indices (where 0 is the first index). ▪ For a detailed description of the individual parameters in this table and for configuring this table using the Web interface, see

Parameter	Description
	"Configuring IP2IP Routing Table (SAS)" on page 163. ▪ For a description on configuring *ini* file table parameters, see "Configuring ini File Table Parameters" on page 194.

10.14 Auxiliary and Configuration Files Parameters

This subsection describes the device's auxiliary and configuration files parameters.

10.14.1 Auxiliary/Configuration File Name Parameters

The configuration files (i.e., auxiliary files) can be loaded to the device using the Web interface or a TFTP session (see "Loading Auxiliary Files" on page 170). 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 a detailed description of the auxiliary files, see "Auxiliary Configuration Files" on page 217.

Table 10-63: Auxiliary and Configuration File Parameters

Parameter	Description
General Parameters	
[SetDefaultOnIniFileProcess]	Determines if all the device's parameters are set to their defaults before processing the updated *ini* file. ▪ **[0]** Disable - parameters not included in the downloaded *ini* file are not returned to default settings (i.e., retain their current settings). ▪ **[1]** Enable (default) **Note:** This parameter is applicable only for automatic HTTP update or Web *ini* file upload (not applicable if the *ini* file is loaded using BootP).
[SaveConfiguration]	Determines if the device's configuration (parameters and files) is saved to flash (non-volatile memory). ▪ **[0]** = Configuration isn't saved to flash memory. ▪ **[1]** = Configuration is saved to flash memory (default).
Auxiliary and Configuration File Name Parameters	
Web/EMS: Call Progress Tones File **[CallProgressTonesFilename]**	The name of the file containing the Call Progress Tones definitions. Refer to the *Product Reference Manual* for additional information on how to create and load this file. **Note:** For this parameter to take effect, a device reset is required.
Web/EMS: Prerecorded Tones File **[PrerecordedTonesFileName]**	The name (and path) of the file containing the Prerecorded Tones. **Note:** For this parameter to take effect, a device reset is required.
[UserInfoFileName]	The name (and path) of the file containing the User Information data.

10.14.2 Automatic Update Parameters

The automatic update of software and configuration files parameters are described in the table below.

Table 10-64: Automatic Update of Software and Configuration Files Parameters

Parameter	Description
General Automatic Update Parameters	
[AutoUpdateCmpFile]	Enables or disables the Automatic Update mechanism for the cmp file. ▪ **[0]** = The Automatic Update mechanism doesn't apply to the cmp file (default). ▪ **[1]** = The Automatic Update mechanism includes the cmp file. **Note:** For this parameter to take effect, a device reset is required.
[AutoUpdateFrequency]	Determines the number of minutes the device waits between automatic updates. The default value is 0 (i.e., the update at fixed intervals mechanism is disabled). **Note:** For this parameter to take effect, a device reset is required.
[AutoUpdatePredefinedTime]	Schedules an automatic update to a user-defined time of the day. The format of this parameter is: 'HH:MM', where *HH* depicts the hour and *MM* the minutes, for example, 20:18. **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ The actual update time is randomized by five minutes to reduce the load on the Web servers.
EMS: AUPD Verify Certificates **[AUPDVerifyCertificates]**	Determines whether the Automatic Update mechanism verifies server certificates when using HTTPS. ▪ **[0]** = Disable (default) ▪ **[1]** = Enable
[AUPDCheckIfIniChanged]	Determines whether the Automatic Update mechanism performs CRC checking to determine if the *ini* file has changed prior to processing. ▪ **[0]** = Do not check CRC. The *ini* file is loaded whenever the server provides it. (default) ▪ **[1]** = Check CRC for the entire file. Any change, including line order, causes the *ini* file to be re-processed. ▪ **[2]** = Check CRC for individual lines. Use this option when the HTTP server scrambles the order of lines in the provided *ini* file.
[ResetNow]	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. ▪ **[0]** = The immediate restart mechanism is disabled (default). ▪ **[1]** = The device immediately resets after an *ini* file with this parameter set to 1 is loaded.

Parameter	Description
Software/Configuration File URL Path for Automatic Update Parameters	
[CmpFileURL]	Specifies the name of the *cmp* file and the path to the server (IP address or FQDN) from where the device loads a new *cmp* file and updates itself. The *cmp* file can be loaded using HTTP/HTTPS, FTP, FTPS, or NFS. For example: http://192.168.0.1/filename **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ When this parameter is configured, the device always loads the *cmp* file after it is reset. ▪ The *cmp* file is validated before it's burned to flash. The checksum of the *cmp* file is also compared to the previously burnt checksum to avoid unnecessary resets. ▪ The maximum length of the URL address is 255 characters.
[IniFileURL]	Specifies the name of the *ini* file and the path to the server (IP address or FQDN) on which it is located. The *ini* file can be loaded using HTTP/HTTPS, FTP, FTPS, or NFS. For example: http://192.168.0.1/filename http://192.8.77.13/config<MAC> https://<username>:<password>@<IP address>/<file name> **Notes:** ▪ For this parameter to take effect, a device reset is required. ▪ When using HTTP or HTTPS, the date and time of the *ini* file are validated. Only more recently dated *ini* files are loaded. ▪ The optional string '<MAC>' is replaced with the device's MAC address. Therefore, the device requests an *ini* file name that contains its MAC address. This option allows the loading of specific configurations for specific devices. ▪ The maximum length of the URL address is 99 characters.
[PrtFileURL]	Specifies the name of the Prerecorded Tones 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. **Note:** The maximum length of the URL address is 99 characters.
[CptFileURL]	Specifies the name of the CPT 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. **Note:** The maximum length of the URL address is 99 characters.
[TLSRootFileUrl]	Specifies the name of the TLS trusted root certificate file and the URL from where it's downloaded. **Note:** For this parameter to take effect, a device reset is required.
[TLSCertFileUrl]	Specifies the name of the TLS certificate file and the URL from where it's downloaded. **Note:** For this parameter to take effect, a device reset is required.
[UserInfoFileURL]	Specifies 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 **Note:** The maximum length of the URL address is 99 characters.

11 SIP Software Package

The table below lists the device's standard SIP software package.

Table 11-1: Software Package

File Name	Description
Firmware (RAM CMP) File	
MP124_SIP_<sw ver.>.cmp	Image file containing the software for MP-124/FXS
MP118_SIP_<sw ver.>.cmp	Common Image file Image file containing the software for MP-11x
ini Configuration Files	
SIPgw_fxs_MP112.ini	Sample ini file for MP-112/FXS
SIPgw_fxs_MP114.ini	Sample ini file for MP-114/FXS
SIPgw_fxo_MP114.ini	Sample ini file for MP-114/FXO
SIPgw_fxs_fxo_MP114.ini	Sample ini file for MP-114/FXS/FXO
SIPgw_fxs_MP118.ini	Sample ini file for MP-118/FXS
SIPgw_fxo_MP118.ini	Sample ini file for MP-118/FXO
SIPgw_fxs_fxo_MP118.ini	Sample ini file for MP-118/FXS/FXO
SIPgw_fxs_MP124.ini	Sample ini file for MP-124/FXS
usa_tones_xx.dat	Default loadable Call Progress Tones *.dat file
usa_tones_xx.ini	Call Progress Tones ini file (used to create *.dat file)
Miscellaneous Files	
SNMP MIBs	MIB library for SNMP browser
Utilities	
DConvert	TrunkPack Downloadable Conversion Utility - to create Call Progress Tones files
ACSyslog	Syslog server
BootP/TFTP Server	BootP/TFTP configuration utility
CPTWizard	Call Progress Tones Wizard

Note: The device is supplied with a cmp file pre-installed on its flash memory. However, if you are an AudioCodes registered customer, you can obtain the latest cmp version files (as well as documentation and other software such as the *ini* and MIB files, and Utilities) from AudioCodes Web site at www.audiocodes.com/downloads (customer registration is performed online at this Web site). If you are not a direct customer of AudioCodes, please contact the AudioCodes' Distributor and Reseller from whom this product was purchased.

Reader's Notes

12 Selected Technical Specifications

The main technical specifications of the MP-11x and MP-124 devices are listed in the table below.

Note: All specifications in this document are subject to change without prior notice.

Table 12-1: MediaPack Technical Specifications

Function	Specification
Interfaces	
Voice Ports	▪ MP-112: 2 ports ▪ MP-114: 4 ports ▪ MP-118: 8 ports ▪ MP-124: 24 ports
Telephone Interfaces	▪ MP-112: FXS, RJ-11 ▪ MP-114 & MP-118: FXS, FXO or mixed FXS/FXO, RJ-11 ▪ MP-124: FXS, 50-pin Telco
Lifeline	Automatic cut through of a single analog line (FXS version only, refers only for the middle column – 4/8 ports)
Network Interface	10/100Base-TX, RJ-45
Indicators Channel	Status and activity LEDs
Voice, Fax, Modem	
Voice over Packet Capabilities	G.168-2004 compliant Echo Cancellation, VAD, CNG, Dynamic programmable Jitter Buffer, modem detection and auto switch to PCM
Voice Compression	G.711, G.723.1, G.726, G.729A, EG.711, G.722
Fax over IP	T.38 compliant Group 3 fax relay up to 14.4 kbps with automatic switching to PCM or ADPCM
3-Way Conference	3-Way conference with local mixing
QoS	DiffServ, TOS, 802.1 P/Q VLAN tagging
IP Transport	RTP/RTCP per IETF RFC 3550 and 3551 PPPoE, Multiplexing (aggregated RTP streams of several channels for saving network bandwith)

Function	Specification
Signaling	
Signaling	▪ MP-112: FXS Loop-start ▪ MP-114 & MP-118: FXS, FXO Loop-start ▪ MP-124: FXS Loop-start
In-band Signaling	DTMF (TIA 464B) User-defined and call progress tones
Out-of-Band Signaling	DTMF Relay (RFC 2833), DTMF via SIP INFO
Control	SIP (RFC 3261)
Provisioning	
Protocols	▪ BootP, DHCP, TFTP and HTTP for Automatic Installation ▪ DHCP options 66,67 in auto update mode ▪ Remote management using Web browser ▪ EMS (Element Management System) / SNMP V3 ▪ Syslog support ▪ RS-232 for basic configuration (via CLI) ▪ Voice Menu using touch-tone phone (FXS interface) for basic configuration
Security	
Media	SRTP
Control	H.235, IPSec, TLS/SIPS
Management	HTTPS, Access List, IPSec
Physical	
Power	Single universal power supply 100-240V 0.3A max. 50-60 Hz or -48V DC **Note:** -48V DC is supported only on MP-124D.
Environmental	Operational: 5 to 40°C (41 to 104°F) Storage: -25 to 85°C (-13 to 185°F) Humidity: 10 to 90% non-condensing
Dimensions	▪ MP-112: 42 x 172 x 220 mm ▪ MP-114 & MP-118: 42 x 172 x 220 mm ▪ MP-124: 44 x 445 x 269 mm
Mounting	Rack mount, Table top, Wall mount
Additional Features	
Message Waiting Indication	Applying 100V DC online for lighting bulb in handset, FSK, Stutter Dial Tone
High Availability	PSTN Fallback: Support of PSTN fallback due to Power failure, if the IP connection is down or due to customer defined IP QoS thresholds Stand Alone Survivability (SAS): Supports SAS of up to 25 SIP users (UA)
Ring voltage	Sine: 54 V RMS typical (balanced ringing only)
Ring Frequency	25-100Hz
Maximum Ringer Load	Ringer Equivalency Number (REN) 3

Function	Specification
Loop Impedance (including phone impedance)	Up to 1500 ohm for the MP-11x, Up to 1600 ohm for the MP-124
Lifeline	Supported in all ports of Mixed FXS/FXO and in first port of MP-114/FXS and MP-118/FXS using special Lifeline cable
Caller ID	Bellcore GR-30-CORE Type 1 using Bell 202 FSK modulation, ETSI Type 1, NTT, Denmark, India, Brazil, British and DTMF ETSI CID (ETS 300-659-1)
Polarity Reversal / Wink	Immediate or smooth to prevent erroneous ringing
Metering Tones	12/16 KHz sinusoidal bursts, Generation on FXS
Distinctive Ringing	By frequency (15-100 Hz) and cadence patterns
Message Waiting Indication	DC voltage generation (TIA/EIA-464-B), V23 FSK data, Stutter dial tone
Outdoor Protection	Over-voltage protection and surge immunity **Note:** Supported only on MP-124D.
Homologation	
EMC	EN55022 Class B , CFR Part 15 Class B, EN55024, EN61000-3-3, EN61000-3-2, VCCI Class X1 (equals to class B)
Safety	EN60950-1 Safety of information technology equipment, UL60950-1 Including compliance to section 6 (over voltage protection).
Telecom	TRR-21, TIA-968

AudioCodes

User's Manual Ver. 6.2

www.audiocodes.com