

Mediant™ 600 & Mediant™ 1000

VoIP Media Gateways

SIP Protocol

User's Manual


HD VoIP
Sounds Better


SAS
Stand Alone Survivability
Continuous VoIP Service



Version 6.4

November 2011

Document # LTRT-83309

 **AudioCodes**

Table of Contents

1	Overview	17
1.1	Mediant 600	17
1.2	Mediant 1000	18
1.3	SIP Overview	20
Part I: Getting Started.....		21
2	Assigning the VoIP LAN IP Address.....	23
2.1	Using CLI	23
2.2	Using the Web Interface.....	25
2.3	Using BootP/TFTP Server.....	26
2.4	Using the FXS Voice Menu Guidance.....	28
Part II: Management Tools		31
3	Web-Based Management.....	33
3.1	Getting Acquainted with the Web Interface.....	33
3.1.1	Computer Requirements.....	33
3.1.2	Accessing the Web Interface.....	34
3.1.3	Areas of the GUI	35
3.1.4	Toolbar Description.....	36
3.1.5	Navigation Tree	37
3.1.5.1	Displaying Navigation Tree in Basic and Full View.....	38
3.1.5.2	Showing / Hiding the Navigation Pane.....	39
3.1.6	Working with Configuration Pages	40
3.1.6.1	Accessing Pages.....	40
3.1.6.2	Viewing Parameters	40
3.1.6.3	Modifying and Saving Parameters	42
3.1.6.4	Entering Phone Numbers.....	43
3.1.6.5	Working with Tables.....	44
3.1.7	Searching for Configuration Parameters	48
3.1.8	Working with Scenarios	49
3.1.8.1	Creating a Scenario.....	49
3.1.8.2	Accessing a Scenario.....	51
3.1.8.3	Editing a Scenario	52
3.1.8.4	Saving a Scenario to a PC.....	53
3.1.8.5	Loading a Scenario to the Device	54
3.1.8.6	Deleting a Scenario	54
3.1.8.7	Quitting Scenario Mode.....	55
3.1.9	Creating a Login Welcome Message.....	56
3.1.10	Getting Help.....	57
3.1.11	Logging Off the Web Interface.....	58
3.2	Using the Home Page	59
3.2.1	Assigning a Port Name.....	62
3.2.2	Resetting an Analog Channel.....	62
3.2.3	Viewing Analog Port Information	62
3.2.4	Viewing Trunk Channels.....	63
3.2.5	Replacing Modules	64
3.3	Configuring Web User Accounts	66
3.4	Configuring Web Security Settings	69

3.5	Web Login Authentication using Smart Cards	70
3.6	Configuring Web and Telnet Access List	70
3.7	Configuring RADIUS Settings	72
4	CLI-Based Management.....	73
4.1	Configuring Telnet and SSH Settings	74
5	SNMP-Based Management.....	75
5.1	Configuring SNMP Community Strings	75
5.2	Configuring SNMP Trap Destinations	76
5.3	Configuring SNMP Trusted Managers	77
5.4	Configuring SNMP V3 Users.....	78
6	EMS-Based Management.....	81
7	INI File-Based Management.....	83
7.1	INI File Format	83
7.1.1	Configuring Individual ini File Parameters	83
7.1.2	Configuring ini File Table Parameters	84
7.1.3	General ini File Formatting Rules	85
7.2	Modifying an ini File	86
7.3	Secured Encoded ini File	86
Part III: General System Settings		87
8	Configuring Certificates	89
8.1	Replacing Device Certificate	89
8.2	Loading a Private Key	92
8.3	Mutual TLS Authentication	93
8.4	Self-Signed Certificates.....	94
9	Date and Time.....	95
9.1	Configuring Manual Date and Time	95
9.2	Configuring Automatic Date and Time through SNTP Server	95
Part IV: VoIP Configuration.....		99
10	Network.....	101
10.1	Ethernet Interface Configuration	101
10.2	Ethernet Interface Redundancy	102
10.3	Configuring IP Interface Settings	102
10.3.1	Network Configuration	106
10.3.1.1	Multiple Network Interfaces and VLANs.....	107
10.3.1.2	Setting Up VoIP Networking.....	114
10.4	Configuring the IP Routing Table	118
10.4.1	Routing Table Columns	120
10.4.1.1	Destination Column	120
10.4.1.2	Prefix Length Column.....	120
10.4.1.3	Gateway Column.....	120
10.4.1.4	Interface Column	121
10.4.1.5	Metric Column	121

10.4.1.6	State Column.....	121
10.4.2	Routing Table Configuration Summary and Guidelines	121
10.4.3	Troubleshooting the Routing Table	122
10.5	Configuring QoS Settings.....	122
10.6	DNS.....	123
10.6.1	Configuring the Internal DNS Table.....	123
10.6.2	Configuring the Internal SRV Table.....	124
10.7	NAT (Network Address Translation) Support.....	125
10.7.1	STUN	126
10.7.2	First Incoming Packet Mechanism.....	127
10.7.3	No-Op Packets	127
10.8	Configuring NFS Settings.....	127
10.9	Robust Receipt of Media Streams	129
10.10	Multiple Routers Support.....	130
10.11	IP Multicasting.....	130
11	Security	131
11.1	Configuring Firewall Settings	131
11.2	Configuring General Security Settings	135
11.3	Configuring IP Security Proposal Table	135
11.4	Configuring IP Security Associations Table	137
12	Media	141
12.1	Configuring Voice Settings.....	141
12.1.1	Voice Gain (Volume) Control.....	141
12.1.2	Silence Suppression (Compression)	142
12.1.3	Echo Cancellation.....	142
12.2	Fax and Modem Capabilities.....	143
12.2.1	Fax/Modem Operating Modes	144
12.2.2	Fax/Modem Transport Modes	144
12.2.2.1	T.38 Fax Relay Mode	144
12.2.2.2	G.711 Fax / Modem Transport Mode	145
12.2.2.3	Fax Fallback.....	146
12.2.2.4	Fax/Modem Bypass Mode	146
12.2.2.5	Fax / Modem NSE Mode.....	147
12.2.2.6	Fax / Modem Transparent with Events Mode	148
12.2.2.7	Fax / Modem Transparent Mode.....	148
12.2.2.8	RFC 2833 ANS Report upon Fax/Modem Detection	149
12.2.3	V.34 Fax Support.....	149
12.2.3.1	Bypass Mechanism for V.34 Fax Transmission.....	149
12.2.3.2	Relay Mode for T.30 and V.34 Faxes	150
12.2.4	V.152 Support.....	150
12.2.5	Fax Transmission behind NAT	151
12.3	Configuring RTP/RTCP Settings.....	152
12.3.1	Configuring Dynamic Jitter Buffer Operation	153
12.3.2	Comfort Noise Generation	154
12.3.3	Dual-Tone Multi-Frequency Signaling	154
12.3.3.1	Configuring DTMF Transport Types.....	154
12.3.3.2	Configuring RFC 2833 Payload	156
12.3.4	Configuring RTP Multiplexing (ThroughPacket)	157
12.3.5	Configuring RTP Base UDP Port.....	158
12.3.6	Configuring RTP Control Protocol Extended Reports (RTCP XR).....	159
12.4	Configuring IP Media Settings.....	160

12.4.1	Answer Machine Detector (AMD)	160
12.4.2	Configuring Automatic Gain Control (AGC)	164
12.5	Configuring General Media Settings	165
12.6	Configuring Analog Settings	166
12.7	Configuring DSP Templates	166
12.7.1	DSP Channel Resources for SBC/IP-to-IP/IP Media Functionality	167
12.7.1.1	Software Upgrade Keys	167
12.7.1.2	Hardware Configuration	168
12.7.1.3	ini File Configuration	169
12.8	Configuring Media Realms	170
12.9	Configuring Media Security	172
12.10	Configuring Quality of Experience Parameters per Media Realm	172
12.11	Configuring Server for Media Quality of Experience	175
13	Services	177
13.1	Routing Based on LDAP Active Directory Queries	177
13.1.1	LDAP Overview	177
13.1.2	Configuring LDAP Settings	178
13.1.3	AD-Based Tel-to-IP Routing in Microsoft OCS 2007 Environment	179
13.2	Least Cost Routing	181
13.2.1	Overview	181
13.2.2	Configuring LCR	184
13.2.2.1	Enabling the LCR Feature	184
13.2.2.2	Configuring Cost Groups	186
13.2.2.3	Configuring Time Bands for Cost Groups	187
13.2.2.4	Assigning Cost Groups to Routing Rules	188
14	Control Network	189
14.1	Configuring SRD Table	189
14.2	Configuring SIP Interface Table	191
14.3	Configuring IP Groups	193
14.4	Configuring Proxy Sets Table	198
14.5	Configuring NAT Translation per IP Interface	202
14.6	Multiple SIP Signaling and Media Interfaces using SRDs	204
15	Enabling Applications	211
16	Coders and Profiles	213
16.1	Configuring Coders	213
16.2	Configuring Coder Groups	214
16.3	Configuring Tel Profile	215
16.4	Configuring IP Profiles	217
17	SIP Definitions	221
17.1	Configuring SIP General Parameters	221
17.2	Configuring Advanced Parameters	222
17.3	Configuring Account Table	223
17.4	Configuring Proxy and Registration Parameters	226
18	GW and IP to IP	229
18.1	Digital PSTN	229
18.1.1	Configuring TDM Bus Settings	229

18.1.2	Configuring CAS State Machines	229
18.1.3	Configuring Trunk Settings	232
18.1.4	Configuring Digital Gateway Parameters	235
18.1.5	Tunneling Applications.....	236
18.1.5.1	TDM Tunneling.....	236
18.1.5.2	QSIG Tunneling.....	239
18.1.6	Advanced PSTN Configuration.....	240
18.1.6.1	Release Reason Mapping	240
18.1.6.2	ISDN Overlap Dialing	244
18.1.6.3	ISDN Non-Facility Associated Signaling (NFAS)	246
18.1.6.4	Redirect Number and Calling Name (Display)	248
18.2	Trunk Group	249
18.2.1	Configuring Trunk Group Table	249
18.2.2	Configuring Trunk Group Settings	251
18.3	Manipulation.....	254
18.3.1	Configuring General Settings	254
18.3.2	Configuring Number Manipulation Tables	254
18.3.3	Configuring Redirect Number IP to Tel.....	258
18.3.4	Configuring Redirect Number Tel to IP.....	260
18.3.5	Mapping NPI/TON to SIP Phone-Context	262
18.3.6	Numbering Plans and Type of Number	264
18.3.7	Configuring Release Cause Mapping.....	265
18.3.8	SIP Calling Name Manipulations	266
18.3.9	SIP Message Manipulation	266
18.3.10	Manipulating Number Prefix	267
18.4	Routing.....	268
18.4.1	Configuring General Routing Parameters	268
18.4.2	Configuring Outbound IP Routing Table.....	269
18.4.3	Configuring Inbound IP Routing Table	277
18.4.4	Configuring Alternative Routing Reasons.....	279
18.4.5	Mapping PSTN Release Cause to SIP Response	280
18.4.6	Configuring Call Forward upon Busy Trunk.....	281
18.5	DTMF and Supplementary	282
18.5.1	Configuring DTMF and Dialing	282
18.5.2	Configuring Supplementary Services	283
18.5.2.1	Call Hold and Retrieve	285
18.5.2.2	BRI Suspend and Resume.....	287
18.5.2.3	Consultation Feature.....	287
18.5.2.4	Call Transfer.....	288
18.5.2.5	Call Forward.....	289
18.5.2.6	Call Waiting	292
18.5.2.7	Message Waiting Indication	293
18.5.2.8	Caller ID	294
18.5.2.9	Three-Way Conferencing	297
18.5.2.10	Emergency E911 Phone Number Services.....	298
18.5.2.11	Multilevel Precedence and Preemption.....	304
18.5.2.12	Denial of Collect Calls	307
18.5.3	Configuring ISDN Supplementary Services.....	307
18.5.4	Configuring Voice Mail Parameters	309
18.5.5	Advice of Charge Services for Euro ISDN.....	310
18.6	Analog Gateway	311
18.6.1	Configuring Keypad Features.....	311
18.6.2	Configuring Metering Tones	312
18.6.3	Configuring Charge Codes	314
18.6.4	Configuring FXO Settings.....	315
18.6.5	Configuring Authentication	316

18.6.6	Configuring Automatic Dialing	317
18.6.7	Configuring Caller Display Information	318
18.6.8	Configuring Call Forward	319
18.6.9	Configuring Caller ID Permissions.....	320
18.6.10	Configuring Call Waiting	321
18.6.11	Configuring FXS Distinctive Ringing and Call Waiting Tones per Source/Destination Number	322
18.6.12	FXS/FXO Coefficient Types.....	323
18.6.13	FXO Operating Modes.....	323
18.6.13.1	FXO Operations for IP-to-Tel Calls	323
18.6.13.2	FXO Operations for Tel-to-IP Calls	326
18.6.13.3	Call Termination on FXO Devices.....	328
18.6.14	Remote PBX Extension Between FXO and FXS Devices.....	329
18.6.14.1	Dialing from Remote Extension (Phone at FXS).....	330
18.6.14.2	Dialing from PBX Line or PSTN	330
18.6.14.3	Message Waiting Indication for Remote Extensions.....	331
18.6.14.4	Call Waiting for Remote Extensions.....	331
18.6.14.5	FXS Gateway Configuration.....	332
18.6.14.6	FXO Gateway Configuration	333
18.7	Dialing Plan Features.....	334
18.7.1	Digit Mapping.....	334
18.7.2	External Dial Plan File	335
18.7.2.1	Modifying ISDN-to-IP Calling Party Number	337
18.7.3	Dial Plan Prefix Tags for IP-to-Tel Routing.....	338
18.8	Configuring Alternative Routing (Based on Connectivity and QoS)	340
18.8.1	Alternative Routing Mechanism.....	340
18.8.2	Determining the Availability of Destination IP Addresses.....	340
18.8.3	PSTN Fallback.....	341
18.9	SIP Call Routing Examples	341
18.9.1	SIP Call Flow Example	341
18.9.2	SIP Message Authentication Example	344
18.9.3	Establishing a Call between Two Devices.....	346
18.9.4	Trunk-to-Trunk Routing Example	347
18.9.5	SIP Trunking between Enterprise and ITSPs.....	348
18.10	IP-to-IP Routing Application.....	351
18.10.1	Theory of Operation.....	352
18.10.1.1	Proxy Sets	353
18.10.1.2	IP Groups	353
18.10.1.3	Inbound and Outbound IP Routing Rules	354
18.10.1.4	Accounts.....	355
18.10.2	IP-to-IP Routing Configuration Example.....	356
18.10.2.1	Step 1: Enable the IP-to-IP Capabilities.....	358
18.10.2.2	Step 2: Configure the Number of Media Channels	358
18.10.2.3	Step 3: Define a Trunk Group for the Local PSTN.....	359
18.10.2.4	Step 4: Configure the Proxy Sets.....	359
18.10.2.5	Step 5: Configure the IP Groups	361
18.10.2.6	Step 6: Configure the Account Table	364
18.10.2.7	Step 7: Configure IP Profiles for Voice Coders	365
18.10.2.8	Step 8: Configure Inbound IP Routing	367
18.10.2.9	Step 9: Configure Outbound IP Routing.....	368
18.10.2.10	Step 10: Configure Destination Phone Number Manipulation.....	370
19	Stand-Alone Survivability (SAS) Application.....	371
19.1	Overview	371
19.1.1	SAS Operating Modes.....	371
19.1.1.1	SAS Outbound Mode	372
19.1.1.2	SAS Redundant Mode.....	373

19.1.2	SAS Routing	375
19.1.2.1	SAS Routing in Normal State	375
19.1.2.2	SAS Routing in Emergency State	377
19.2	SAS Configuration.....	378
19.2.1	General SAS Configuration	378
19.2.1.1	Enabling the SAS Application	378
19.2.1.2	Configuring Common SAS Parameters	379
19.2.2	Configuring SAS Outbound Mode	381
19.2.3	Configuring SAS Redundant Mode	382
19.2.4	Configuring Gateway Application with SAS.....	382
19.2.4.1	Gateway with SAS Outbound Mode.....	383
19.2.4.2	Gateway with SAS Redundant Mode.....	384
19.2.5	Advanced SAS Configuration	386
19.2.5.1	Manipulating URI user part of Incoming REGISTER	386
19.2.5.2	Manipulating Destination Number of Incoming INVITE.....	387
19.2.5.3	SAS Routing Based on SAS Routing Table.....	389
19.2.5.4	Blocking Calls from Unregistered SAS Users	392
19.2.5.5	Configuring SAS Emergency Calls	392
19.2.5.6	Adding SIP Record-Route Header to SIP INVITE	394
19.2.5.7	Replacing Contact Header for SIP Messages	395
19.3	Viewing Registered SAS Users.....	396
19.4	SAS Cascading	396
20	Configuring the IP Media Parameters.....	399
20.1	Overview	399
20.1.1	Conference Server.....	400
20.1.1.1	Simple Conferencing (NetAnn)	401
20.1.1.2	Advanced Conferencing (MSCML)	403
20.1.1.3	Conference Call Flow Example.....	408
20.1.2	Announcement Server.....	414
20.1.2.1	NetAnn Interface	414
20.1.2.2	MSCML Interface	415
20.1.2.3	Voice Streaming.....	424
20.1.2.4	Announcement Call Flow Example	435
20.1.3	Voice XML Interpreter.....	438
20.1.3.1	Features	438
20.1.3.2	Feature Key.....	438
20.1.3.3	VXML Scripts.....	438
20.1.3.4	Proprietary Extensions	439
20.1.3.5	Combining <audio> Elements	445
20.1.3.6	Notes Regarding Non-compliant Functionality.....	445
20.1.3.7	Supported Elements and Attributes	445
20.1.3.8	Example of UDT 'beep' Tone Definition	460
20.1.3.9	Limitations and Restrictions	460
21	Transcoding using Third-Party Call Control.....	461
21.1	Using RFC 4117.....	461
21.2	Using RFC 4240 - NetAnn 2-Party Conferencing	462
Part V: Maintenance		465
22	Basic Maintenance.....	467
22.1	Resetting the Device	467
22.2	Locking and Unlocking the Device	469

22.3	Saving Configuration.....	470
23	Software Upgrade.....	471
23.1	Loading Auxiliary Files	471
23.1.1	Call Progress Tones File	474
23.1.1.1	Distinctive Ringing.....	477
23.1.2	Prerecorded Tones File	479
23.1.3	Voice Prompts File.....	479
23.1.4	CAS Files.....	480
23.1.5	Dial Plan File.....	480
23.1.6	User Information File	482
23.1.6.1	User Information File for PBX Extensions and "Global" Numbers.....	482
23.1.7	AMD Sensitivity File.....	483
23.2	Loading Software Upgrade Key	485
23.2.1	Loading via BootP/TFTP.....	487
23.3	Software Upgrade Wizard.....	488
23.4	Backing Up and Loading Configuration File.....	491
24	Restoring Factory Defaults	493
24.1	Restoring Defaults using CLI	493
24.2	Restoring Defaults using Hardware Reset Button.....	494
24.3	Restoring Defaults using an ini File.....	494
Part VI: Status, Performance Monitoring and Reporting.....		495
25	System Status	497
25.1	Viewing Device Information.....	497
25.2	Viewing Ethernet Port Information	498
26	Carrier-Grade Alarms.....	499
26.1	Viewing Active Alarms.....	499
26.2	Viewing Alarm History	500
27	Performance Monitoring.....	501
27.1	Viewing Trunk Utilization.....	501
27.2	Viewing MOS per Media Realm	503
28	VoIP Status	505
28.1	Viewing Active IP Interfaces.....	505
28.2	Viewing Performance Statistics.....	505
28.3	Viewing Call Counters.....	506
28.4	Viewing SAS/SBC Registered Users	508
28.5	Viewing Call Routing Status.....	508
28.6	Viewing Registration Status	509
28.7	Viewing IP Connectivity.....	510
29	Reporting Information to External Party	513
29.1	Generating Call Detail Records.....	513
29.1.1	CDR Fields for Gateway Application	513
29.1.2	Release Reasons in CDR.....	515
29.1.3	Supported RADIUS Attributes	517

29.2	Event Notification using X-Detect Header	520
29.3	Querying Device Channel Resources using SIP OPTIONS	522
Part VII: Diagnostics.....		523
30	Configuring Syslog Settings	525
31	Viewing Syslog Messages.....	527
Part VIII: Appendices.....		529
A	Configuration Parameters Reference	531
A.1	Networking Parameters.....	531
A.1.1	Ethernet Parameters.....	531
A.1.2	Multiple Network Interfaces and VLAN Parameters	532
A.1.3	Static Routing Parameters.....	534
A.1.4	Quality of Service Parameters.....	535
A.1.5	NAT and STUN Parameters	536
A.1.6	NFS Parameters	538
A.1.7	DNS Parameters.....	539
A.1.8	DHCP Parameters	540
A.1.9	NTP and Daylight Saving Time Parameters.....	541
A.2	Management Parameters.....	542
A.2.1	General Parameters	542
A.2.2	Web Parameters.....	542
A.2.3	Telnet Parameters	544
A.2.4	SNMP Parameters.....	545
A.2.5	Serial Parameters	548
A.3	Debugging and Diagnostics Parameters.....	549
A.3.1	General Parameters	549
A.3.2	Syslog, CDR and Debug Parameters.....	551
A.3.3	Resource Allocation Indication Parameters.....	554
A.3.4	BootP Parameters	554
A.4	Security Parameters.....	556
A.4.1	General Parameters	556
A.4.2	HTTPS Parameters	557
A.4.3	SRTP Parameters.....	559
A.4.4	TLS Parameters.....	561
A.4.5	SSH Parameters.....	563
A.4.6	IPSec Parameters.....	564
A.4.7	OCSP Parameters	565
A.5	RADIUS Parameters	566
A.6	SIP Media Realm Parameters.....	567
A.7	Quality of Experience Reporting	568
A.8	Control Network Parameters.....	569
A.8.1	IP Group, Proxy, Registration and Authentication Parameters	569
A.8.2	Network Application Parameters	580
A.9	General SIP Parameters	582
A.10	Coders and Profile Parameters.....	608
A.11	Channel Parameters	617
A.11.1	Voice Parameters	617
A.11.2	Coder Parameters	619

A.11.3	DTMF Parameters	621
A.11.4	RTP, RTCP and T.38 Parameters.....	622
A.12	Gateway and IP-to-IP Parameters	627
A.12.1	Fax and Modem Parameters	627
A.12.2	DTMF and Hook-Flash Parameters.....	632
A.12.3	Digit Collection and Dial Plan Parameters.....	637
A.12.4	Voice Mail Parameters.....	639
A.12.5	Supplementary Services Parameters	644
A.12.5.1	Caller ID Parameters.....	644
A.12.5.2	Call Waiting Parameters.....	649
A.12.5.3	Call Forwarding Parameters	651
A.12.5.4	Message Waiting Indication Parameters.....	653
A.12.5.5	Call Hold Parameters	655
A.12.5.6	Call Transfer Parameters	656
A.12.5.7	Three-Way Conferencing Parameters	658
A.12.5.8	Emergency Call Parameters	659
A.12.5.9	Call Cut-Through Parameters	660
A.12.5.10	Automatic Dialing Parameters.....	661
A.12.5.11	Direct Inward Dialing Parameters	662
A.12.5.12	MLPP Parameters.....	664
A.12.5.13	ISDN BRI Parameters	668
A.12.5.14	TTY/TDD Parameters	669
A.12.6	PSTN Parameters.....	670
A.12.6.1	General Parameters	670
A.12.6.2	TDM Bus and Clock Timing Parameters.....	675
A.12.6.3	CAS Parameters	677
A.12.6.4	ISDN Parameters	680
A.12.7	ISDN and CAS Interworking Parameters	686
A.12.8	Answer and Disconnect Supervision Parameters	704
A.12.9	Tone Parameters	708
A.12.9.1	Telephony Tone Parameters.....	708
A.12.9.2	Tone Detection Parameters	712
A.12.9.3	Metering Tone Parameters	714
A.12.10	Telephone Keypad Sequence Parameters.....	715
A.12.11	General FXO Parameters.....	718
A.12.12	FXS Parameters	721
A.12.13	Trunk Groups and Routing Parameters.....	721
A.12.14	Alternative Routing Parameters.....	728
A.12.15	Number Manipulation Parameters.....	732
A.12.16	LDAP Parameters.....	744
A.12.17	Least Cost Routing Parameters	746
A.13	Standalone Survivability Parameters	746
A.14	IP Media Parameters	751
A.15	Auxiliary and Configuration Files Parameters	762
A.15.1	Auxiliary and Configuration File Name Parameters	762
A.15.2	Automatic Update Parameters	764
B	Dialing Plan Notation for Routing and Manipulation.....	767
C	SIP Message Manipulation Syntax.....	769
C.1	Actions	769
C.2	Header Types.....	769
C.2.1	Accept.....	769
C.2.2	Accept-Language.....	770
C.2.3	Allow	770
C.2.4	Call-Id.....	770
C.2.5	Contact.....	771
C.2.6	Cseq.....	771

C.2.7	Diversion.....	772
C.2.8	Event.....	773
C.2.9	From.....	773
C.2.10	History-Info	774
C.2.11	Min-Se and Min-Expires	775
C.2.12	P-Asserted-Identity	776
C.2.13	P-Associated-Uri.....	776
C.2.14	P-Called-Party-Id	777
C.2.15	P-Charging-Vector	778
C.2.16	P-Preferred-Identity	778
C.2.17	Privacy	779
C.2.18	Proxy-Require.....	779
C.2.19	Reason.....	780
C.2.20	Referred-By	781
C.2.21	Refer-To.....	781
C.2.22	Remote-Party-Id	782
C.2.23	Request-Uri.....	783
C.2.24	Require	784
C.2.25	Resource-Priority	785
C.2.26	Retry-After	785
C.2.27	Server or User-Agent.....	786
C.2.28	Service-Route.....	786
C.2.29	Session-Expires.....	787
C.2.30	Subject.....	788
C.2.31	Supported	788
C.2.32	To.....	789
C.2.33	Unsupported	790
C.2.34	Via.....	790
C.2.35	Warning	791
C.2.36	Unknown Header	792
C.3	Structure Definitions.....	793
C.3.1	Event Structure	793
C.3.2	Host.....	793
C.3.3	MLPP	793
C.3.4	Privacy Struct.....	793
C.3.5	Reason Structure.....	794
C.3.6	SIPCapabilities	794
C.3.7	URL.....	795
C.4	Random Type.....	796
C.4.1	Random Strings	796
C.4.2	Random Integers	796
C.5	Wildcarding for Header Removal	796
C.6	Copying Information between Messages using Variables	797
C.7	Enum Definitions	798
C.7.1	AgentRole	798
C.7.2	Event Package.....	798
C.7.3	MLPP Reason Type.....	799
C.7.4	Number Plan.....	799
C.7.5	NumberType	799
C.7.6	Privacy	800
C.7.7	Reason (Diversion)	800
C.7.8	Reason (Reason Structure).....	800
C.7.9	Reason (Remote-Party-Id).....	803
C.7.10	Refresher	803
C.7.11	Screen.....	803
C.7.12	ScreenInd	803
C.7.13	TransportType	804

C.7.14 Type.....	804
C.8 Actions and Types.....	804
C.9 Syntax	809
D DSP Templates	815
D.1 Analog Interfaces	815
D.2 Digital Interfaces	816
D.3 Media Processing Interfaces.....	817
E Selected Technical Specifications.....	819
E.1 Mediant 600	819
E.2 Mediant 1000	820

Notice

This document describes the AudioCodes Mediant 600 and Mediant 1000 Voice-over-IP (VoIP) SIP media 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: November-08-2011

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

Abbreviations and Terminology

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

Related Documentation

Manual Name
SIP CPE Release Notes
Product Reference Manual for SIP CPE Devices
Mediant 600 Hardware Installation Manual
Mediant 1000 Hardware Installation Manual
CPE Configuration Guide for IP Voice Mail



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



Note: Throughout this manual, unless otherwise specified, the term *device* refers to the Mediant 600 and Mediant 1000.



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

1 Overview

This section provides an overview of the Mediant 1000 and Mediant 600 media gateways.

1.1 Mediant 600

The Mediant 600 (hereafter referred to as *device*) is a cost-effective, wireline Voice-over-IP (VoIP) Session Initiation Protocol (SIP)-based media gateway. It is designed to interface between Time-Division Multiplexing (TDM) and IP networks in enterprises, small and medium businesses (SMB), and CPE application service providers. Incorporating AudioCodes' innovative VoIP technology, the device enables rapid time-to-market and reliable cost-effective deployment of next-generation networks.

The device is based on VoIPerfect, AudioCodes underlying, best-of-breed, media gateway core technology. The device provides superior voice technology for connecting legacy telephone and PBX systems to IP networks, as well as seamlessly connecting IP-PBXs to the PSTN. The device also provides SIP trunking capabilities for Enterprises operating with multiple Internet Telephony Service Providers (ITSP) for VoIP services. The device is fully interoperable with multiple vendors of IP-PBXs, IP Centrex application servers, softswitches, gateways, proxy servers, IP phones, Session Border Controllers and firewalls.

The device supports the following interfaces:

- Up to two E1/T1/J1 spans (including fractional E1/T1)
- Up to eight ISDN Basic Rate Interface (BRI) interfaces
- Up to four FXO interfaces (RJ-11 ports) - for connecting analog lines of an enterprise's PBX or the PSTN to the IP network
- Up to four FXS interfaces (RJ-11 ports) - for connecting legacy telephones, fax machines, and modems to the IP network. Optionally, the FXS interfaces can be connected to the external trunk lines of a PBX.

When deployed with a combination of FXO and FXS modules, the device can be used as a PBX for Small Office Home Office (SOHO) users, and businesses not equipped with a PBX. These interfaces can be provided in one of the following configurations:

- 1 x E1/T1 port (can support also Fractional E1/T1)
- 2 x E1/T1 ports
- 4 x BRI ports (supporting up to 8 voice calls)
- 8 x BRI ports (supporting up to 16 voice calls)
- 4 x BRI ports and 1 x E1/T1 port
- 4 x BRI ports and 4 x FXS ports
- 4 x BRI ports and 4 x FXO ports
- 4 x FXS ports and 1 x E1/T1 port
- 4 x FXO ports and 1 x E1/T1 port

The device supports various ISDN PRI protocols such as EuroISDN, North American NI2, Lucent™ 4/5ESS, Nortel™ DMS-100 and others, supporting different variants of CAS protocols, including MFC R2, E&M immediate start, E&M delay dial / start, loop- and ground-start signaling. The device also supports various ISDN BRI protocols such as ETSI 5ESS and QSIG over BRI. The device also provides dual Ethernet 10/100Base-TX ports for IP redundancy.

Intelligently packaged in a stackable 1U chassis, the compact device can be mounted on a desk or in a standard 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 a Web browser (such as Microsoft™ Internet Explorer™).

1.2 Mediant 1000

The Mediant 1000 (hereafter referred to as *device*) is a best-of-breed Voice-over-IP (VoIP) Session Initiation Protocol (SIP) Media Gateway, using field-proven, market-leading technology, implementing analog and digital cutting-edge technology. The device is designed to seamlessly interface between Time-Division Multiplexing (TDM) and Internet Protocol (IP) networks, providing superior voice quality and optimized packet voice streaming (voice, fax, and data traffic) over IP networks.

The device is best suited for small-to-medium sized (SME) enterprises, branch offices, and residential media gateway solutions. The device is a highly scalable and modular system that matches the density requirements for smaller environments, while meeting service providers' demands for growth.

The device is ideal for connecting an enterprise's legacy telephones, fax machines, and Private Branch Exchange (PBX) systems to IP-based telephony networks, as well as for seamlessly connecting IP-based PBX architecture to the Public Switched Telephone Network (PSTN). The device also provides SIP trunking capabilities (including IP-to-IP call routing) for Enterprises operating with multiple Internet Telephony Service Providers (ITSP) for VoIP services. In addition to operating as a pure media gateway, the device incorporates an open platform, known as the Open Solutions Network (OSN) server, allowing additional deployment options by hosting third-party partner VoIP applications such as IP-PBX, Calling Card, and IP-PBX redundancy.

The device also provides conferencing services over VoIP networks. This is supported by an optional Media Processing Module (MPM) that can be housed in the device's chassis. The MPM module also provides IP Media channels for use on various Media Server applications.

The device is fully interoperable with multiple vendor gateways, softswitches, SIP servers, gatekeepers, proxy servers, IP phones, session border controllers (SBC), and firewalls. The device is designed to meet regulatory approval (including Safety, EMC, and Telecom for USA, EU and other countries).

Intelligently packaged in a stackable and compact 1U chassis, it can be mounted on a desk, a wall, or in a standard 19-inch rack. The device is supplied with two integral mounting brackets for facilitating rack installation.

The device is equipped with two 10/100Base-TX Ethernet ports for connection to the IP network. The second Ethernet port is used for 1+1 Ethernet redundancy.

The device supports mixed digital and analog interface configurations:

■ Digital:

- The device supports multiples of 1, 2, or 4 E1/T1/J1 spans for connecting the PSTN/PBX to the IP network. The digital modules provide RJ-48 ports. The digital module can be configured with up to 1 or 2 paired spans for switching to the PSTN in case of power or network failure (PSTN Fallback).
- The device also supports ISDN Basic Rate Interface (BRI) modules for connecting BRI-based PSTN or PBX lines to the IP network. Each BRI module supports four BRI ports (RJ-45). Up to five BRI modules can be housed in the device, supporting up to 20 BRI digital ports. The BRI module can be configured as 'Lifeline' telephone interfaces, switching to the PSTN in case of power failure or network problems.
- Depending on configuration, the device can provide IP Media channels at the expense of PSTN channels. These channels may be used for Media Server applications.

- **Analog:** The device's analog interface supports up to 24 analog ports (four ports per analog module) in various Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) configurations, supporting up to 24 simultaneous VoIP calls. The device supports up to six analog modules, each module providing four analog RJ-11 ports. The FXO module can be used to connect analog lines of an enterprise's PBX or the PSTN to the IP network. The FXS module can be used to connect legacy telephones, fax machines, and modems to the IP network. Optionally, the FXS module can be connected to the external trunk lines of a PBX. When deployed with a combination of FXO and FXS modules, the device can be used as a PBX for Small Office Home Office (SOHO) users, and businesses not equipped with a PBX.
- **Media Processing Module (MPM):** The MPM module provides IP media channels for conferencing and media server functionality. The device can house up to three MPM modules.

The device has enhanced hardware and software capabilities to ease its installation and to maintain voice quality. If the measured voice quality falls beneath a pre-configured value, or the path to the destination is disconnected, the device assures voice connectivity by 'falling' back to the PSTN. In the event of network problems or power failures, calls can be routed back to the PSTN without requiring routing modifications in the PBX. Further reliability is provided by dual Ethernet ports and an optional dual AC power supply.

The device supports various ISDN PRI protocols such as EuroISDN, North American NI2, Lucent™ 4/5ESS, Nortel™ DMS-100 and others. It also supports various ISDN BRI protocols such as ETSI 5ESS and QSIG over BRI. In addition, it supports different variants of CAS protocols for E1 and T1 spans, including MFC R2, E&M immediate start, E&M delay dial / start, loop start and ground start.

The device 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 a Web browser (such as Microsoft™ Internet Explorer™).

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>).



Part I

Getting Started

Before you can begin configuring your device, you need to access it with the default LAN IP address and change this IP address to suit your networking scheme. Once modified, you can then access the device using the new LAN IP address. This section describes how to perform this initialization process.

Reader's Notes

2 Assigning the VoIP LAN IP Address

This section describes how to change the default VoIP LAN IP address so that it corresponds to your networking scheme.

The default VoIP LAN IP address is listed in the table below:

Table 2-1: Default VoIP LAN IP Address

IP Address	Value
IP Address	10.1.10.10
Subnet Mask	255.255.0.0
Default Gateway IP Address	0.0.0.0

You can use any of the following management tools to change the default VoIP LAN IP address:

- Embedded command line interface (CLI) - see 'Using CLI' on page 23
- Embedded HTTP-based Web server - see 'Using the Web Interface' on page 25
- Bootstrap Protocol (BootP) - see Using BootP/TFTP Server on page 26
- Analog (FXS) telephone voice menu - see Using the FXS Voice Menu Guidance on page 28

2.1 Using CLI

The procedure below describes how to assign a VoIP LAN IP address, using CLI.

➤ **To assign a LAN IP address using CLI:**

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

Figure 2-1: Connecting to Serial Port for Initial Connectivity – Mediant 1000

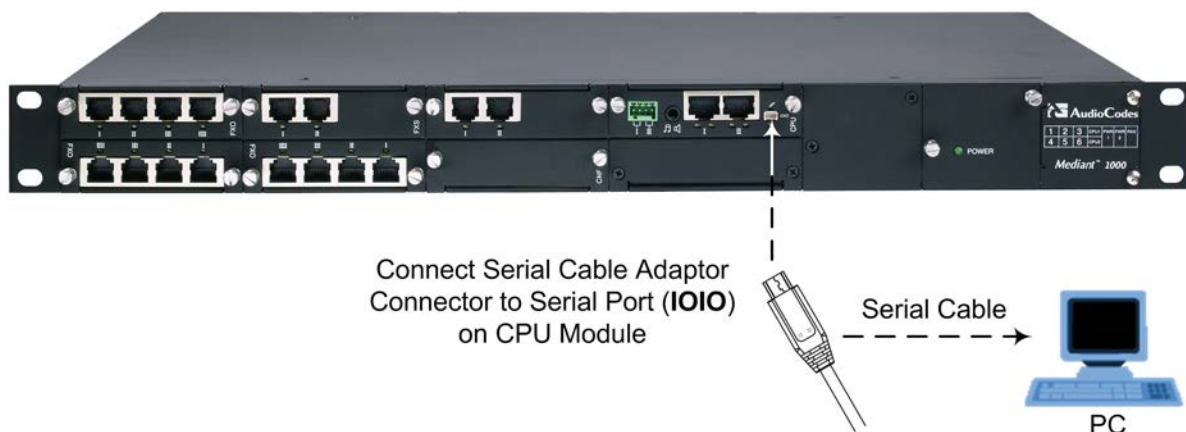
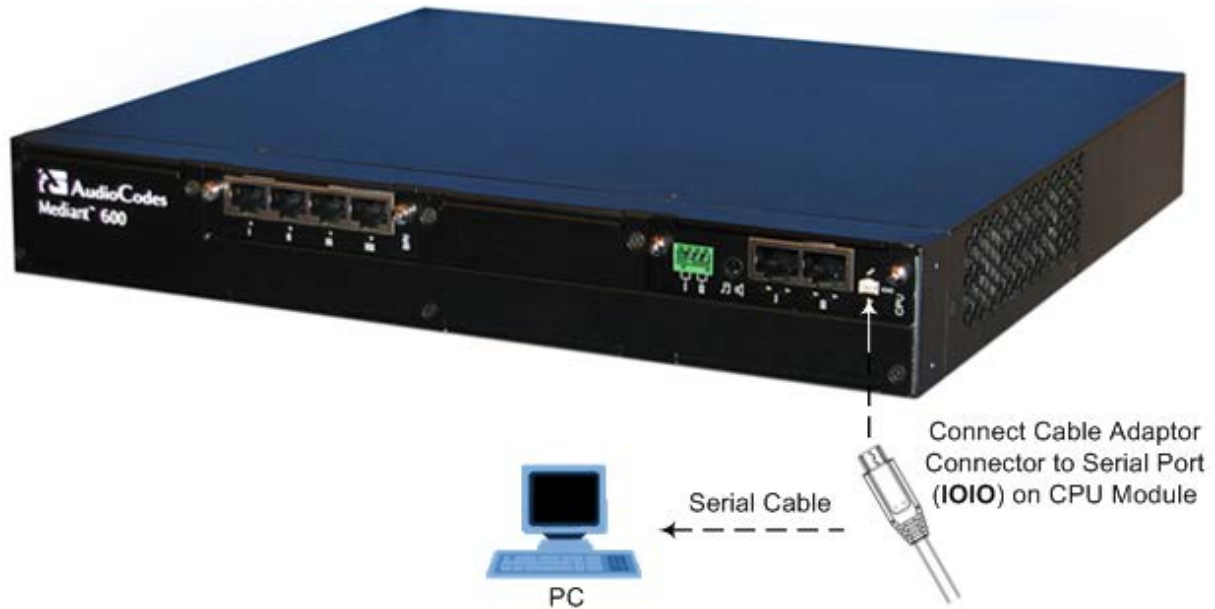


Figure 2-2: Connecting to Serial Port for Initial Connectivity – Mediant 600


2. Establish a serial communication link with the device using a terminal emulator program (such as HyperTerminal) with the following communication port settings:
 - Baud Rate: 115,200 bps
 - Data Bits: 8
 - Parity: None
 - Stop Bits: 1
 - Flow Control: None
3. At the prompt, type the following command to access the configuration folder, and then press Enter:


```
conf
```
4. At the prompt, type the following command to view the current network settings, and then press Enter:


```
GCP IP
```
5. At the prompt, typing the following command to change the network settings, and then press Enter:


```
SCP IP <ip_address> <subnet_mask> <default_gateway>
```

You must enter all three network parameters, each separated by a space, for example:

```
SCP IP 10.13.77.7 255.255.0.0 10.13.0.1
```
6. At the prompt, type the following command to save the settings and reset the device, and then press Enter:


```
SAR
```


2.2 Using the Web Interface

The procedure below describes how to assign a LAN IP address, using the Web interface.

➤ **To assign an IP address using the Web interface:**

1. Disconnect any network cables from the device.
2. Connect one of the LAN ports of the device directly to the network interface of your computer, using a straight-through Ethernet cable.

Figure 2-3: Connecting to LAN for Initial Connectivity – Mediant 1000

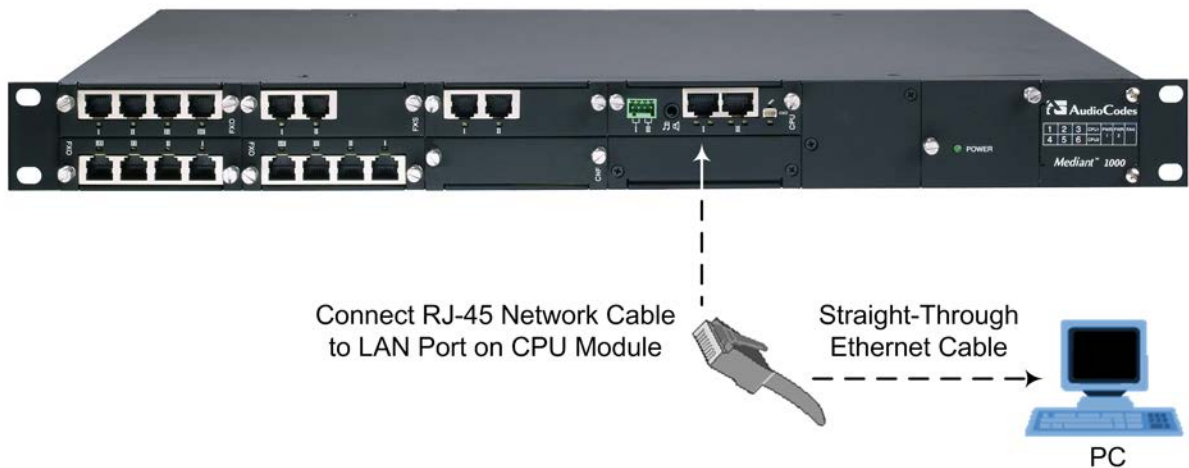
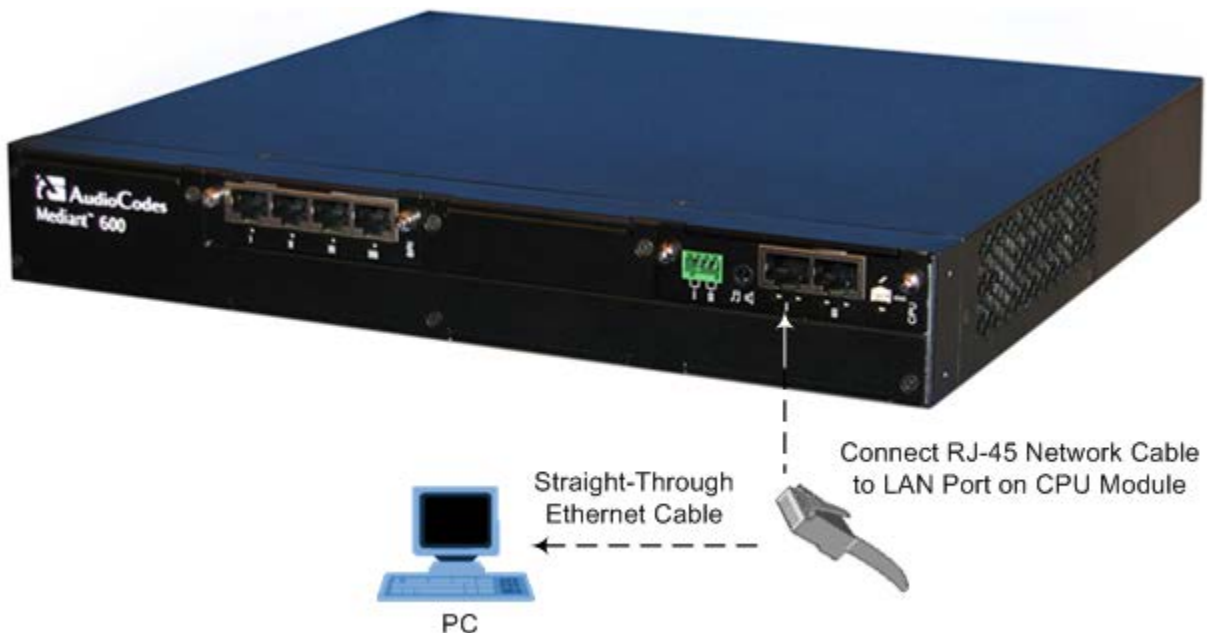


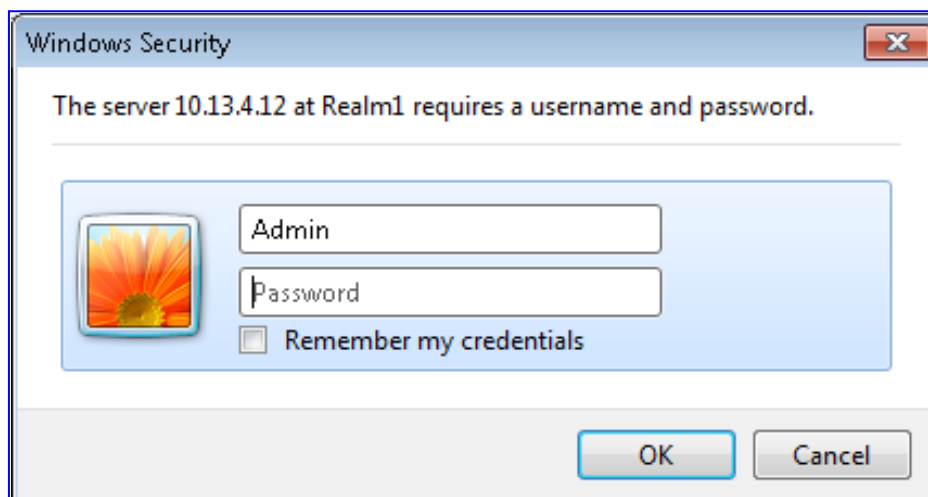
Figure 2-4: Connecting to LAN for Initial Connectivity – Mediant 600



3. Change the IP address and subnet mask of your computer to correspond with the default IP address and subnet mask of the device.

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

Figure 2-5: Login Screen



5. In the 'User Name' and 'Password' fields, enter the default login user name "Admin" (case-sensitive) and password "Admin" (case-sensitive), and then click **OK**; the device's Web interface is accessed.
6. Open the Multiple Interface Table page (**Configuration** tab > **VoIP** menu > **Network** submenu > **IP Settings**).
7. Select the 'Index' radio button corresponding to the "OAMP + Media + Control" application type, and then click **Edit**.
8. Change the IP address, subnet mask, and Default Gateway IP address to correspond with your network IP addressing scheme.
9. Click **Apply**, and then click **Done** to validate your settings.
10. Save your settings to the flash memory with a device reset.
11. Disconnect the computer from the device or hub / switch (depending on the connection used in Step 2) and reconnect the device to your network.

2.3 Using BootP/TFTP Server

You can assign an IP address to the device, using the supplied AudioCodes BootP/TFTP Server utility.



Notes:

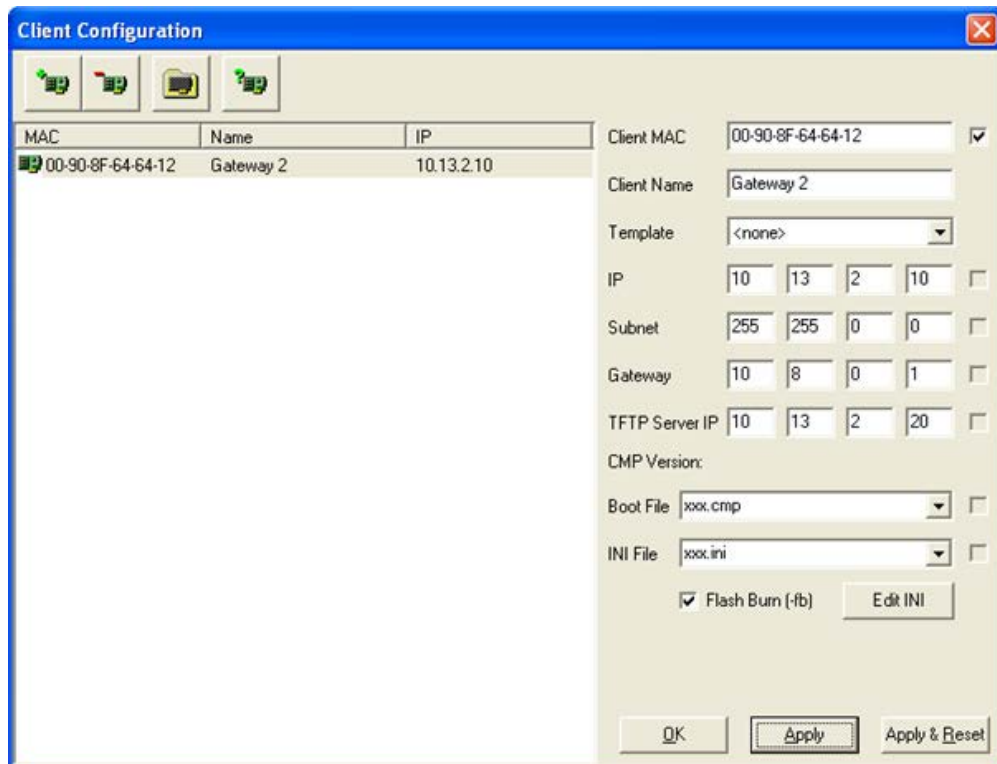
- The BootP procedure can also be done using any standard compatible BootP server.
- For a detailed description of BootP, refer to the *Product Reference Manual*.


➤ **To assign an IP address using BootP:**

1. Start the BootP application.
2. From the **Edit** menu, choose **Preferences**, and then in the Preferences dialog box, set the 'Timeout' field to "50".
3. From the **Services** menu, choose **Clients**; the Client Configuration dialog box appears.

4. Click the **Add New Client**  icon.

Figure 2-6: BootP Client Configuration Screen



MAC	Name	IP
 00-90-8F-64-64-12	Gateway 2	10.13.2.10

Client MAC: 00-90-8F-64-64-12

Client Name: Gateway 2

Template: <none>

IP: 10 | 13 | 2 | 10

Subnet: 255 | 255 | 0 | 0

Gateway: 10 | 8 | 0 | 1

TFTP Server IP: 10 | 13 | 2 | 20

CMP Version:

Boot File: xxx.cmp

INI File: xxx.ini

Flash Burn (-fb)

5. In the 'Client MAC' field, enter the device's MAC address. The MAC address is printed on the label located on the underside of the device. Ensure that the check box to the right of the field is selected in order to enable the client.
6. In the 'IP' field, enter the IP address (in dotted-decimal notation) that you want to assign the device.
7. In the 'Subnet' field, enter the subnet mask (in dotted-decimal notation) that you want to assign the device.
8. In the 'Gateway' field, enter the IP address of the Default Gateway (if required).
9. Click **Apply** to save the new client.
10. Click **OK**; the 'Client Configuration' screen closes.
11. Physically reset the device by powering down and then powering up the device. This enables the device to receive its new networking parameters through the BootP process.

2.4 Using the FXS Voice Menu Guidance

You can assign an IP address that suits your networking scheme using a standard touch-tone telephone connected to one of the FXS ports. The voice menu can also be used to query and modify basic configuration parameters.



Notes:

- Assigning an IP address using the voice menu is applicable only when the device is installed with an FXS module.
- If you want to disable the voice menu, do one of the following:
 - Set the VoiceMenuPassword parameter to 'disable'.
 - Change the Web login password for the Admin user from its default value (i.e., "Admin") to any other value, and then reset the device.

➤ To assign an IP address using the voice menu:

1. Connect a telephone to one of the FXS ports.
2. Lift the handset and dial *****12345** (three stars followed by the digits 1, 2, 3, 4, and 5).
3. Wait for the 'configuration menu' voice prompt to be played.
4. To change the IP address:
 - a. Press **1** followed by the pound key (**#**); the current IP address of the device is played.
 - b. Press the **#** key.
 - c. Dial the new IP address, using the star (*****) key instead of periods (**.**), e.g., 192*168*0*4, and then press **#** to finish.
 - d. Review the new IP address, and then press **1** to save.
5. To change the subnet mask:
 - a. Press **2** followed by the **#** key; the current subnet mask of the device is played.
 - b. Press the **#** key.
 - c. Dial the new subnet mask (e.g., 255*255*0*0), and then press **#** to finish.
 - d. Review the new subnet mask, and then press **1** to save.
6. To change the Default Gateway IP address:
 - a. Press **3** followed by the **#** key; the current Default Gateway address is played.
 - b. Press the **#** key.
 - c. Dial the new Default Gateway address (e.g., 192*168*0*1), and then press **#** to finish.
 - d. Review the new Default Gateway address, and then press **1** to save.
7. Hang up (on-hook) the handset.

Alternatively, initial configuration may be performed using an HTTP server, as discussed in the *Product Reference Manual* ('Automatic Update Facility'). The Voice Menu may be used to specify the configuration URL.

➤ **To set a configuration URL:**

1. Obtain the IP address of the configuration HTTP server (e.g., 36.44.0.6).
2. Connect a telephone to one of the FXS ports.
3. Lift the handset and dial *****12345** (three stars followed by the digits 1, 2, 3, 4, and 5).
4. Wait for the 'configuration menu' voice prompt to be played.
5. Dial **31** followed by the **#** key; the current IP address is played.
6. To change the IP address:
 - a. Press the **#** key.
 - b. Dial the configuration server's IP address. Use the star (*) key instead of dots ("."), e.g., 36*44*0*6, and then press **#** to finish.
 - c. Review the configuration server's IP address, and then press **1** to save.
7. Dial **32** followed by the **#** key, and then do the following to change the configuration file name pattern:
 - a. Press the **#** key.
 - b. Select one of the patterns listed in the table below (*aa.bb.cc.dd* denotes the IP address of the configuration server):

#	Configuration File Name Pattern	Description
1	http://aa.bb.cc.dd/config.ini	Standard config.ini.
2	https://aa.bb.cc.dd/config.ini	Secure HTTP.
3	http://aa.bb.cc.dd/audiocodes/<MAC>.ini	The device's MAC address is appended to the file name (e.g., http://36.44.0.6/audiocodes/00908f012300.ini).
4	http://aa.bb.cc.dd:8080/config.ini	HTTP on port 8080.
5	http://aa.bb.cc.dd:1400/config.ini	HTTP on port 1400.
6	http://aa.bb.cc.dd/cgi-bin/acconfig.cgi?mac=<MAC>&ip=<IP>	Generating configuration per IP/MAC address dynamically, using a CGI script. See perl example below.

- a. Press the selected pattern code, and then press **#** to finish.
8. Press **1** to save, and then hang up the handset. The device retrieves the configuration from the HTTP server.

The following is an example perl CGI script, suitable for most Apache-based HTTP servers for generating configuration dynamically per pattern #6 above. Copy this script to `/var/www/cgi-bin/acconfig.cgi` on your Apache server and edit it as required:

```
#!/usr/bin/perl
use CGI;
$query = new CGI;
$mac = $query->param('mac');
$ip = $query->param('ip');
print "Content-type: text/plain\n\n";
print "; INI file generator CGI\n";
print "; Request for MAC=$mac IP=$ip\n\n";
print <<"EOF";
SyslogServerIP = 36.44.0.15
EnableSyslog = 1
SSHServerEnable = 1
EOF
```

The table below lists the configuration parameters that can be viewed and modified using the voice menu:

Table 2-2: Configuration Parameters Available via the Voice Menu

Item Number at Menu Prompt	Description
1	IP address.
2	Subnet mask.
3	Default Gateway IP address.
4	Primary DNS server IP address.
7	DHCP enable / disable.
31	Configuration server IP address.
32	Configuration file name pattern.
99	Voice menu password (initially 12345). Note: The voice menu password can also be changed using the Web interface or <i>ini</i> file parameter <code>VoiceMenuPassword</code> (refer to the <i>User's Manual</i>).



Part II

Management Tools

This part provides an overview of the various management tools that can be used to configure the device and describes how to configure the management settings. The following management tools can be used to configure the device:

- Embedded HTTP/S-based Web server - see 'Web-based Management' on page [33](#)
- Command Line Interface (CLI) - see 'CLI-Based Management' on page [73](#)
- Configuration *INI* file - see 'INI File-Based Management' on page [83](#)
- AudioCodes Element Management System - see 'EMS-Based Management' on page [81](#)
- Simple Network Management Protocol (SNMP) browser software - see 'SNMP-Based Management' on page [75](#)



Notes:

- Some configuration settings can only be done using specific management tools. For example, the *ini* file method provides many parameters that are not supported in the Web interface.
- The CLI is used only for debugging.
- If you use AudioCodes BootP/TFTP utility to assign an IP address to the device (see Using BootP/TFTP Server on page [26](#)), you can also in the same process load a firmware file (.cmp) and a configuration ini file (.ini file). For more information on using the BootP/TFTP utility, refer to the Product Reference Manual.

Reader's Notes

3 Web-Based Management

The device's embedded Web server (hereafter referred to as the *Web interface*) provides FCAPS (fault management, configuration, accounting, performance, and security) functionality. The Web interface allows you to remotely configure the device for quick-and-easy deployment, including the loading of software (.cmp), configuration (.ini), and auxiliary files. The Web interface provides real-time, online monitoring of the device, including display of alarms and their severity. In addition, the Web interface 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 529.
- 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 529.
- 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 529.
- 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 485.



3.1 Getting Acquainted with the Web Interface

This section provides a description of the Web interface, including the areas of the GUI, navigation, and configuration methods.

3.1.1 Computer Requirements

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

- A network connection to the device.
- One of the following Web browsers:
 - Microsoft™ Internet Explorer™ (version 6.0 or later)
 - Mozilla Firefox® (versions 2 or 3)
- The following 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 procedure below describes how to access the Web interface.
When initially accessing the Web interface, use

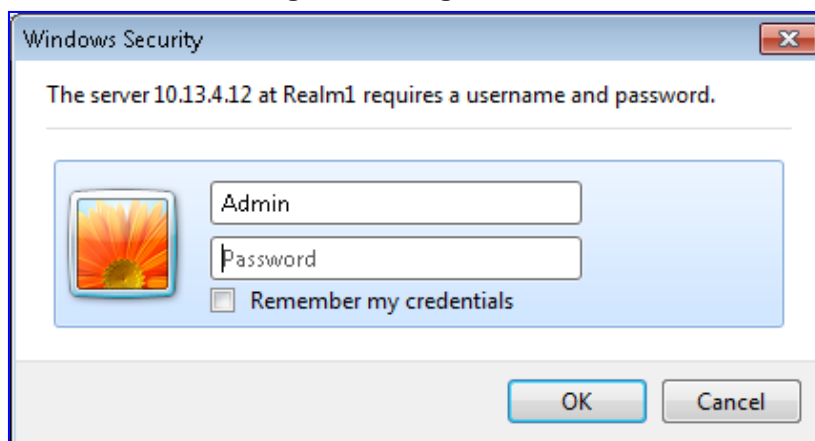


Note: For assigning an IP address to the device, refer to the *Installation Manual*.

➤ **To access the Web interface:**

1. Open a standard Web browser (see 'Computer Requirements' on page 33).
2. In the Web browser, specify the IP address of the device (e.g., `http://10.1.10.10`); the Web interface's Login window appears, as shown below:

Figure 3-1: Login Screen



3. In the 'User Name' and 'Password' fields, enter the case-sensitive, user name and password respectively.



Notes:

- The default user name and password is "Admin". To change the login user name and password, see 'Configuring the Web User Accounts' on page 66.
- If you want the Web browser to remember your password, select the 'Remember my credentials' check box. The next time you log in to the Web interface, instead of entering your credentials as described in Step 3 above, all you need to do is to click **OK** twice in succession.

4. Click **OK**; the Web interface is accessed, displaying the Home page (for a detailed description of the Home page, see 'Using the Home Page' on page 59).



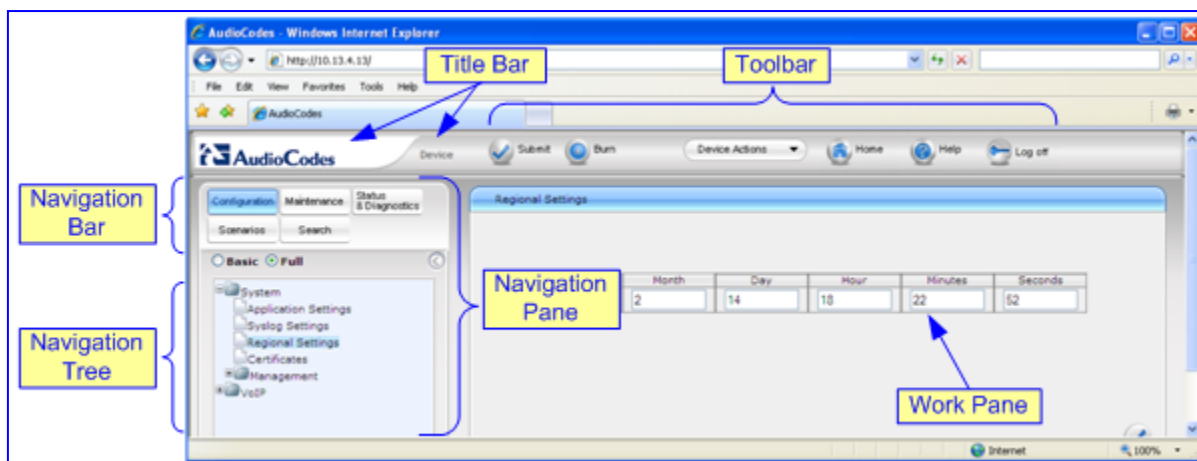
Note: If access to the Web interface is denied ("Unauthorized") due to Microsoft Internet Explorer security settings, do the following:

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 the Web browser and start it again.

3.1.3 Areas of the GUI

The figure below displays the areas of the Web interface GUI:

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









The Web GUI consists of the following main areas:

- **Title bar:** Displays the corporate logo image and product name.
- **Toolbar:** Provides frequently required command buttons (see 'Toolbar Description' on page 36).
- **Navigation Pane:** Includes the following areas:
 - **Navigation bar:** Provides tabs for accessing the configuration menus (see 'Navigation Tree' on page 37), creating Scenarios (see Scenarios on page 49), and searching Web interface parameters (see 'Searching for Configuration Parameters' on page 48).
 - **Navigation tree:** Displays the elements pertaining to the selected tab on the Navigation bar (tree-like structure of the configuration menus, Scenario Steps, or Search engine).
- **Work pane:** Displays configuration pages in which configuration is done (see 'Working with Configuration Pages' on page 40).

3.1.4 Toolbar Description

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

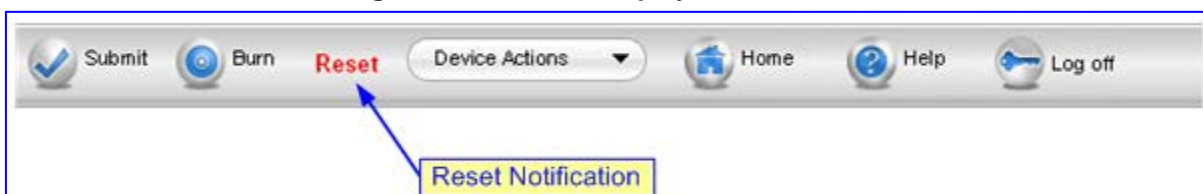
Table 3-1: Description of Toolbar Buttons

Icon	Button Name	Description
	Submit	Applies parameter settings to the device (see 'Saving Configuration' on page 470). 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 470).
	Device Actions	Opens a drop-down menu list with frequently needed commands: <ul style="list-style-type: none"> ▪ Load Configuration File: opens the Configuration File page for loading an <i>ini</i> file (see 'Backing Up and Loading Configuration File' on page 491). ▪ Save Configuration File: opens the Configuration File page for saving the <i>ini</i> file to a folder on a computer (see 'Backing Up and Loading Configuration File' on page 491). ▪ Reset: opens the Maintenance Actions page for resetting the device (see 'Resetting the Device' on page 467). ▪ Software Upgrade Wizard: starts the Software Upgrade wizard for upgrading the device's software (see 'Software Upgrade Wizard' on page 488).
	Home	Opens the Home page (see 'Using the Home Page' on page 59).
	Help	Opens the Online Help topic of the currently opened configuration page (see 'Getting Help' on page 57).
	Log off	Logs off a session with the Web interface (see 'Logging Off the Web Interface' on page 58).



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

Figure 3-3: "Reset" Displayed on Toolbar



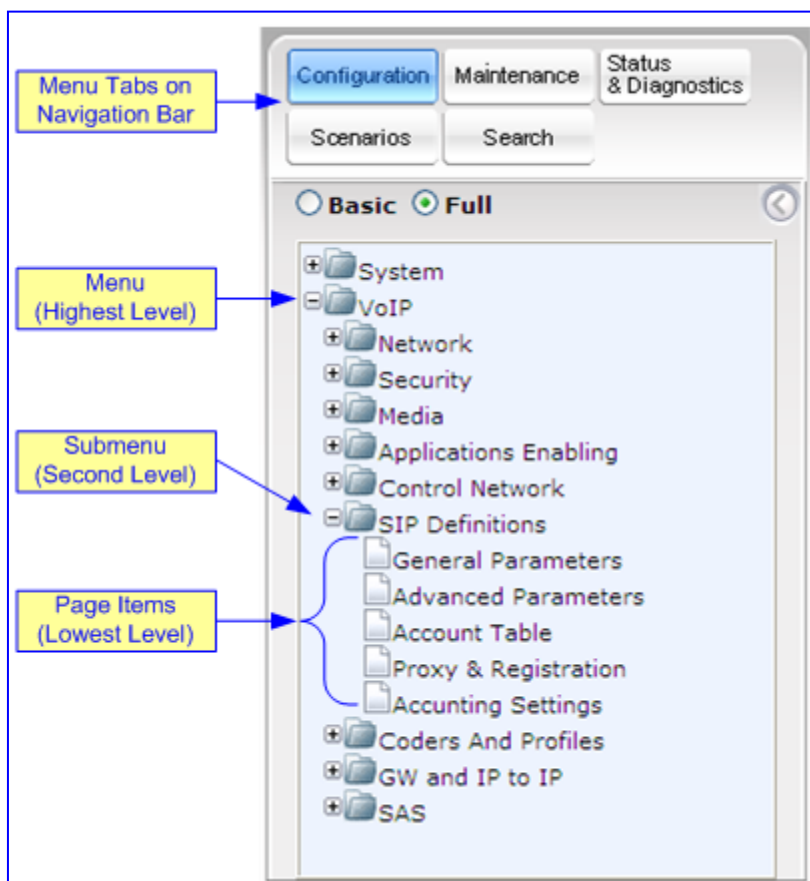
3.1.5 Navigation Tree

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

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

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

Figure 3-4: Terminology for Navigation Tree Levels



➤ **To view menus in the Navigation tree:**

- On the Navigation bar, select the required tab - **Configuration, Maintenance, or Status & Diagnostics.**

➤ **To navigate to a page:**

1. Navigate to the required page item, by performing the following:
 - Drilling-down using the **plus** \oplus sign to expand the menu and submenus.
 - Drilling-up using the **minus** \ominus sign to collapse the menu 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:

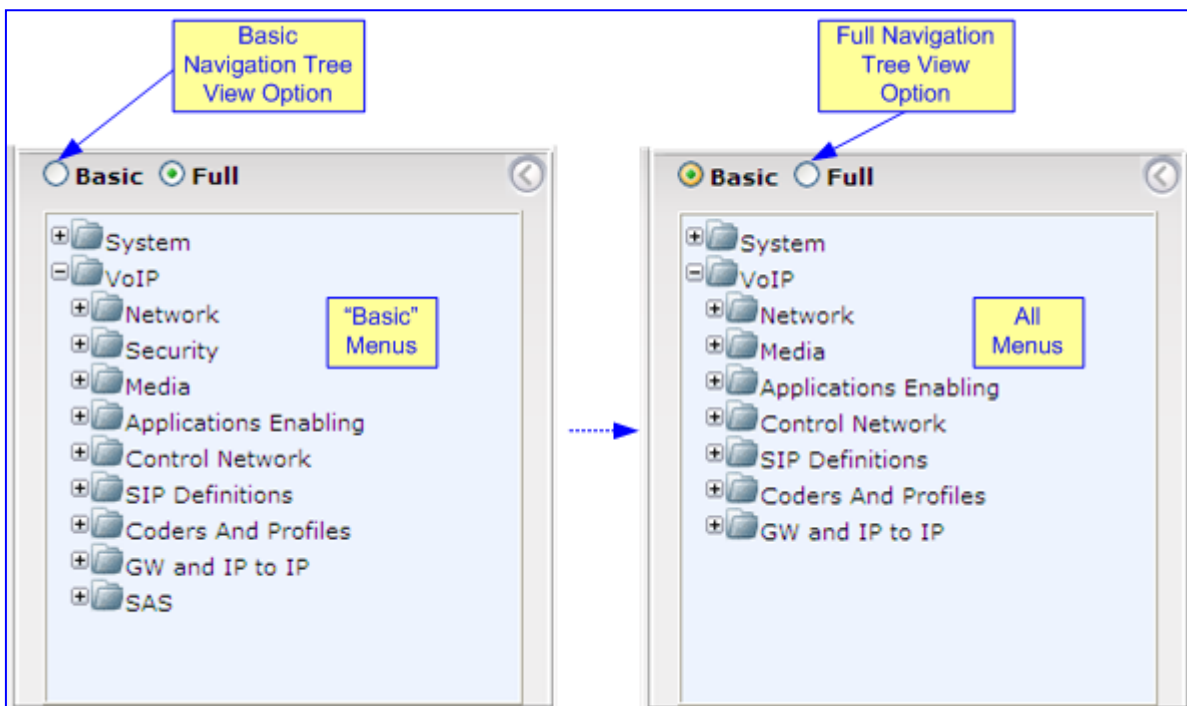
- **Basic:** displays only commonly used menus
- **Full:** displays all the menus pertaining to a configuration tab

The advantage of the Basic view is that it prevents "cluttering" of 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: Navigation Tree in Basic and Full View



Note:

- After you reset the device, the Web GUI is displayed in Basic view.
- When in Scenario mode (see Scenarios on page 49), 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 table that's wider than the Work pane and to view 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.



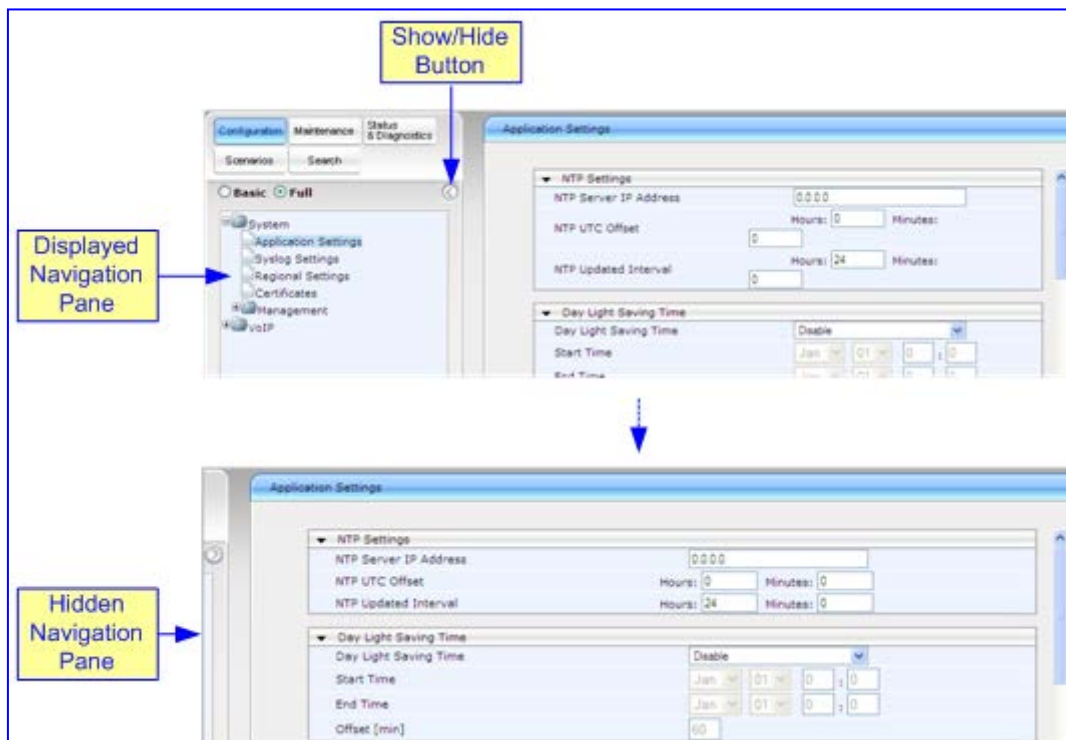
- **To hide the Navigation pane:** click the left-pointing arrow ; the pane is hidden and the button is replaced by the right-pointing arrow button.
- **To show the Navigation pane:** click the right-pointing arrow ; the pane is displayed and the button is replaced by the left-pointing arrow button.

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 and are displayed in the Work pane, 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:**

1. On the Navigation bar, click the required tab:

- **Configuration**
- **Maintenance**
- **Status & Diagnostics**

The menus pertaining to the selected tab appear in the Navigation tree.

2. In the Navigation tree, drill-down to the required submenu and then click the required page item; the page opens in the Work pane.

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

Notes:

- You can also access certain pages from the **Device Actions** button located on the toolbar (see 'Toolbar Description' on page 36).
- 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 38).
- To get Online Help for the currently displayed page, see 'Getting Help' on page 57.
- 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. The Web interface provides two methods for displaying page parameters:

- Displaying "basic" and "advanced" parameters - see 'Displaying Basic and Advanced Parameters' on page 41
- Displaying parameter groups - see 'Showing / Hiding Parameter Groups' on page 42

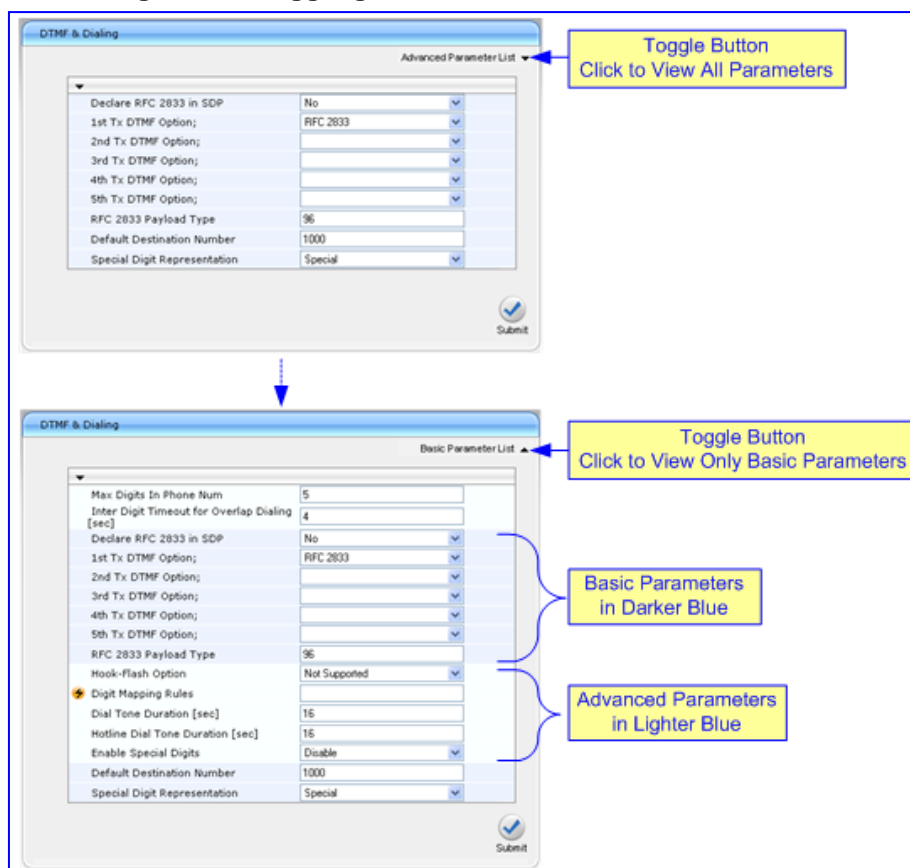
3.1.6.2.1 Displaying Basic and Advanced Parameters

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:

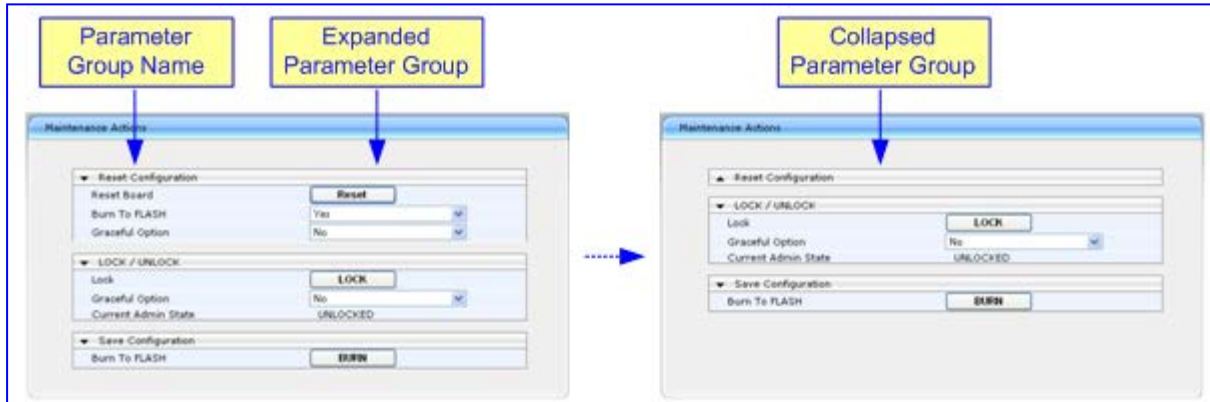
- When the Navigation tree is in Full mode (see 'Navigation Tree' on page 37), configuration pages display all their parameters (i.e., the Advanced Parameter List view is displayed).
- If a page contains only basic parameters, the **Basic Parameter List** button is not displayed.
- After you reset the device, the Web pages display only the basic parameters.



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 title button that appears above each group. The button appears with a down-pointing or up-pointing arrow, indicating that it can be collapsed or expanded when clicked, respectively.

Figure 3-8: Expanding and Collapsing Parameter Groups



3.1.6.3 Modifying and Saving Parameters



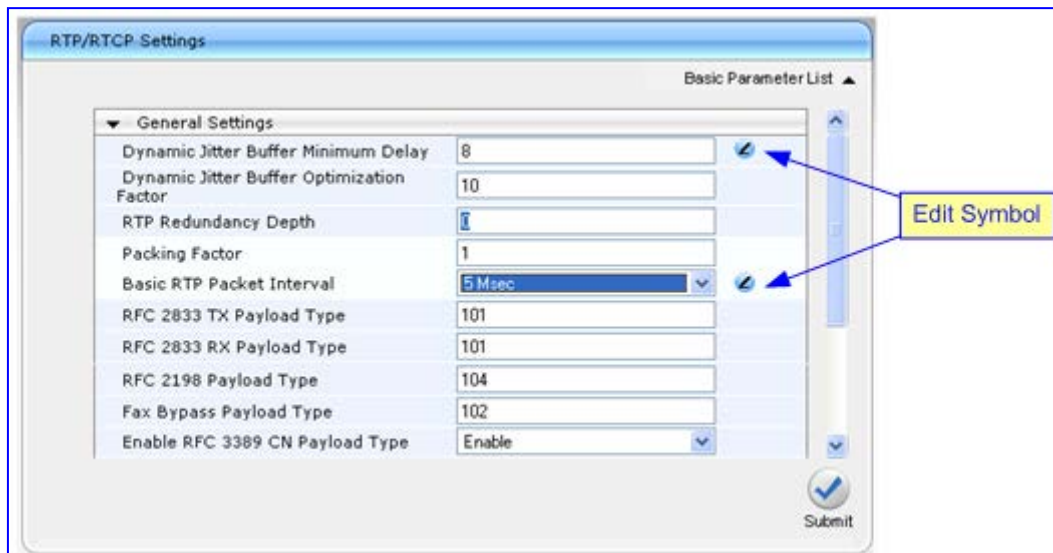


When you modify a parameter value on a page, the **Edit**  symbol appears to the right of the parameter. This is useful for indicating the parameters that you have currently modified (before applying the changes). After you apply your modifications, the  symbols disappear.

Figure 3-9: Edit Symbol after Modifying Parameter Value



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

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

When you click **Submit**, modifications to parameters with on-the-fly capabilities are immediately applied to the device and take effect; 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 467) before taking effect.

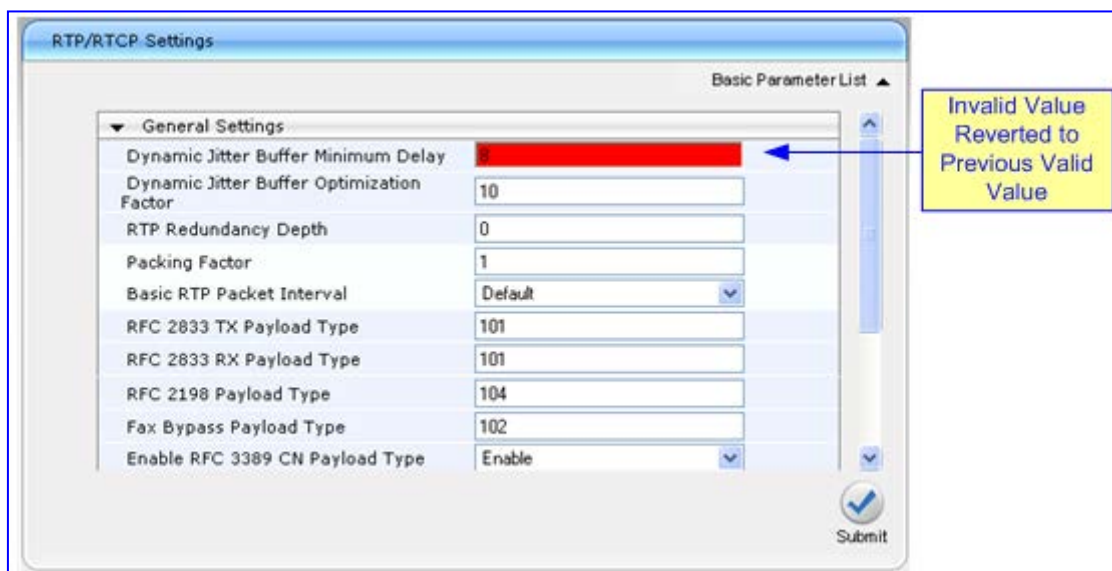
Notes:

- 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, save ('burn') them to the device's non-volatile memory, i.e., flash (see 'Saving Configuration' on page 470).
- 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

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

3.1.6.5.1 Basic Design Tables

The basic design 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

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	QAMP + Media + Control	10.13.4.13	16	10.13.0.1	1	0+M+C

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



Notes:

- Before you can add another index entry, 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 copy 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 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

The figure illustrates the process of compacting a web interface table. It shows two states of the table: one with inconsecutive index numbers and one with compacted, consecutive index numbers.

Inconsecutive Index Numbers:

Index	ApplicationTypes	IPv6InterfaceMode	IPAddress	PrefixLength	Gateway	VlanID	InterfaceName
0	6	0	10.13.4.13	16	10.13.0.1	0	Unknown
2	6	0	10.13.4.10	16	0.0.0.0	2	Unknown
5	6	0	10.13.4.8	16	0.0.0.0	0	ALL

Compacted Table:

Index	ApplicationTypes	IPv6InterfaceMode	IPAddress	PrefixLength	Gateway	VlanID	InterfaceName
0	6	0	10.13.4.13	16	10.13.0.1	0	Unknown
1	6	0	10.13.4.10	16	0.0.0.0	2	Unknown
2	6	0	10.13.4.8	16	0.0.0.0	0	ALL

- **To delete an 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.

3.1.6.5.2 Enhanced Design Tables

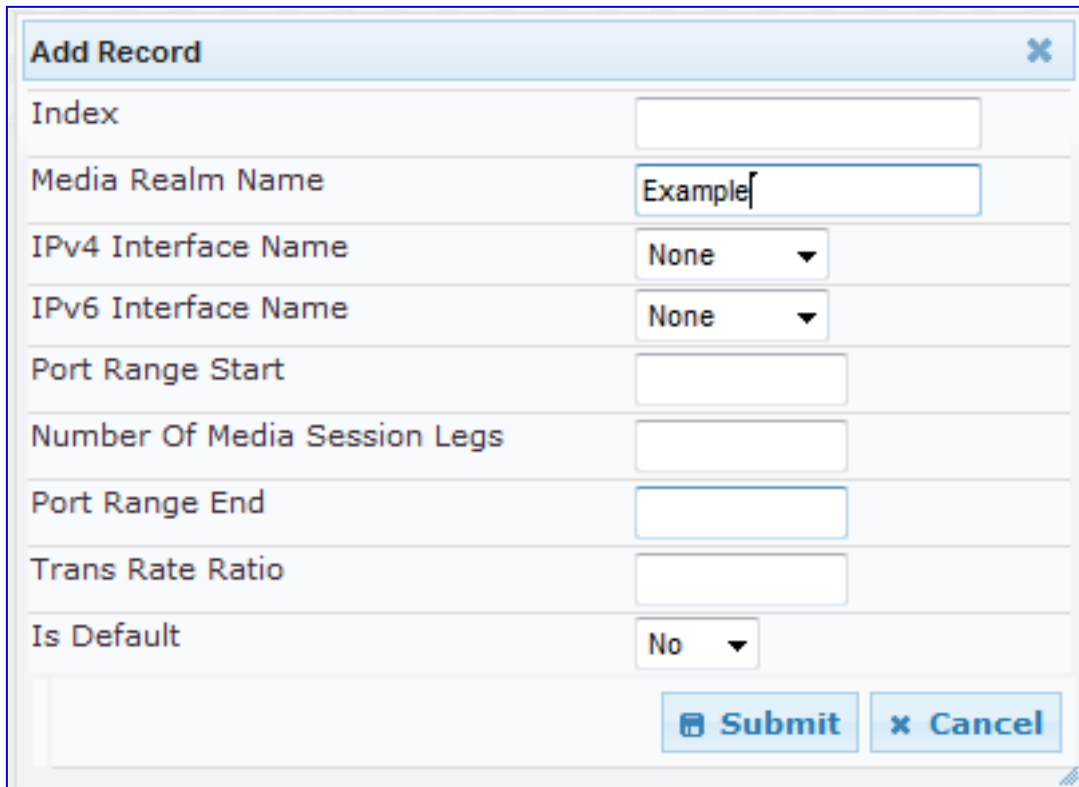
The enhanced table structure includes the following buttons:

- **Add:** adds a row entry to the table
- **Edit:** edits the selected table row
- **Delete:** deletes a selected table row
- **View/Unview:** shows or hides all configuration settings of selected table rows

➤ **To add an entry:**

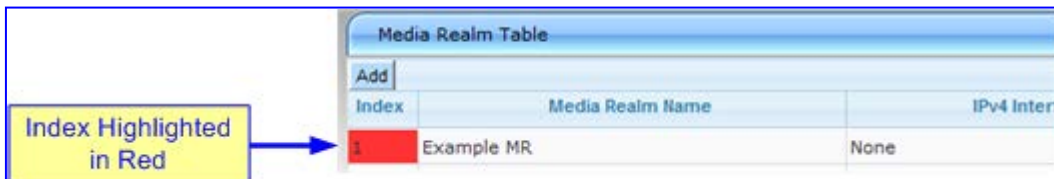
1. Click the **Add** button; the Add Record dialog box appears:

Figure 3-13: Add Record Dialog Box



2. Configure the required parameters, and then click **Submit** to apply your changes (or **Cancel** to ignore your changes); the new row entry is added to the table. If the configuration is invalid, the index of the table row is highlighted in red, as shown below:

Figure 3-14: Index Highlighted in Red

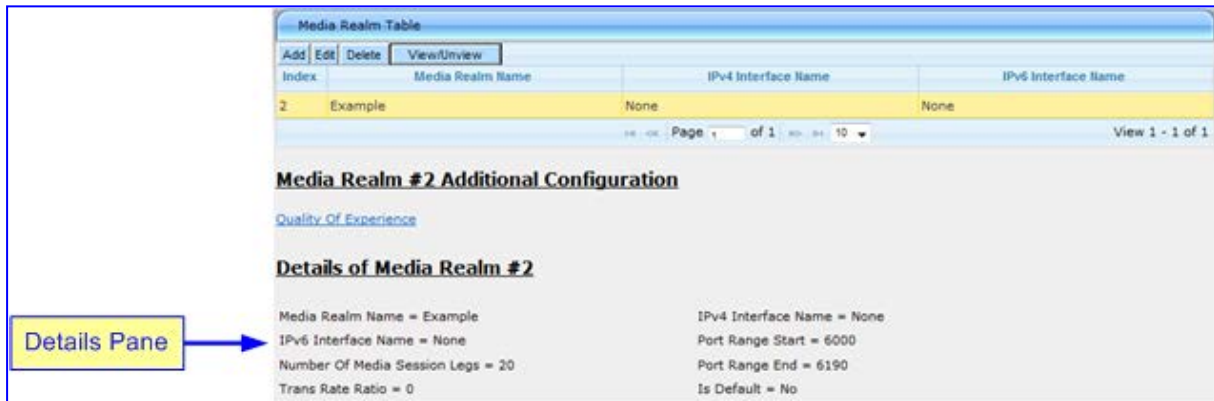


Index	Media Realm Name	IPv4 Interf
1	Example MR	None

By default, the table displays 10 entries per page. However, you can change this to 5 by selecting **5** from the drop-down list located immediately below the table. If your table spans over multiple pages, you can navigate between the pages by clicking the left and right arrow buttons located immediately below the table.

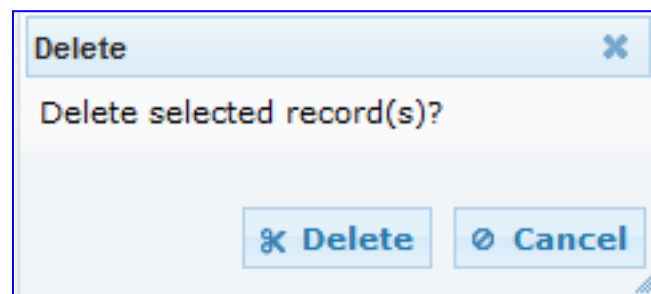
- **To view the configuration settings of an entry:**
- 1. Select the table row that you want to view, and then click the **View/Unview** button; a Details pane appears below the table, displaying the configuration settings of the selected row, as shown below:

Figure 3-15: Displayed Details Pane



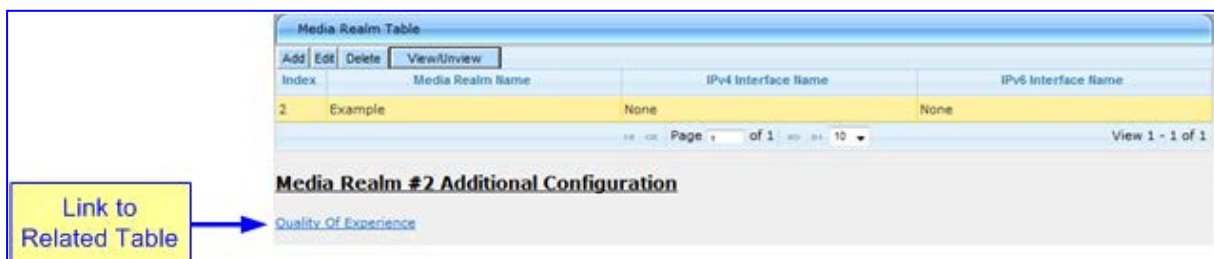
- 2. To hide the Details pane, click the **View/Unview** button again.
- **To edit an entry:**
- 1. Select the table row that you want to modify, and then click the **Edit** button; the Edit Record dialog box appears.
- 2. Make the required changes, and then click **Submit**.
- **To delete an entry:**
- 1. Select the table row that you want to delete, and then click the **Delete** button; the Delete message box appears:

Figure 3-16: Delete Message Box



- 2. Click **Delete** to confirm deletion (or **Cancel** to abort the process).
- Some tables provide a link to a related table for advanced configuration of a selected row entry, as shown below:

Figure 3-17: Link to Related Table



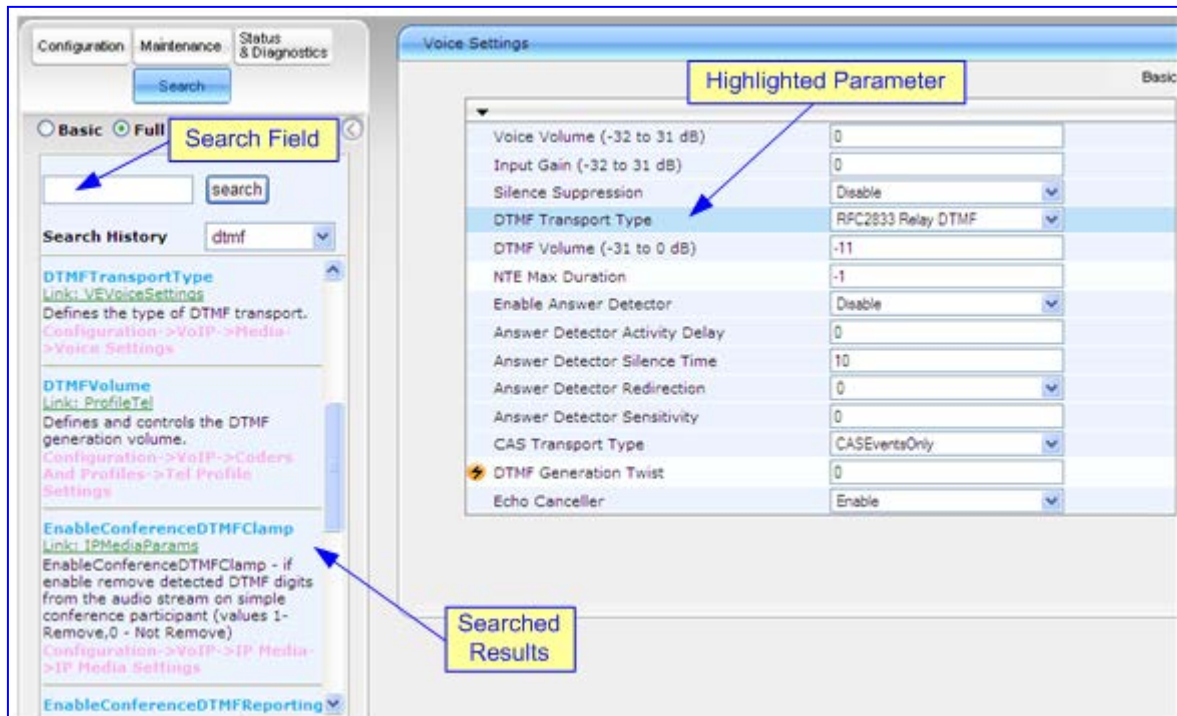
3.1.7 Searching for Configuration Parameters

The Web interface provides a search engine that allows you to search any *ini* file parameter that is configurable in the Web interface (i.e., has a corresponding Web parameter). You can search for a specific parameter (e.g., "EnableIPSec") or a substring of that parameter (e.g., "sec"). If you search for a substring, all parameters containing the searched substring 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 substring of the parameter name that you want to search. If you have done a previous search for such a parameter, instead of entering the required string, you can use the 'Search History' drop-down list to select the string saved from a previous search.
3. Click **Search**; a list of 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 in the page for easy identification, as shown in the figure below:

Figure 3-18: Searched Result Screen



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 54).

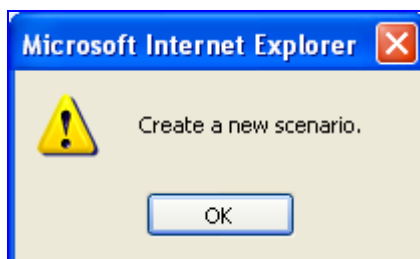
3.1.8.1 Creating a Scenario

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 3-19: 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.

- 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 3-20: Creating a Scenario

The screenshot shows the configuration interface for creating a scenario. The navigation tree on the left is in 'Full' display, with 'DTMF & Dialing' selected. The main area displays a 'Selected Parameter' list with various settings. At the bottom, there are fields for 'Scenario Name' (PBX Interoperability) and 'Step Name' (SIPDDTMF), and a 'Next Button'.

- Repeat steps 5 through 8 to add additional Steps (i.e., pages).
- 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.
- 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 37.
- 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.

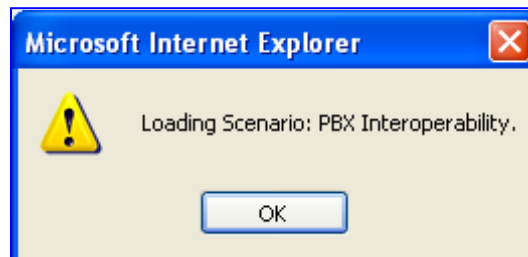
3.1.8.2 Accessing a Scenario

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

➤ **To access the Scenario:**

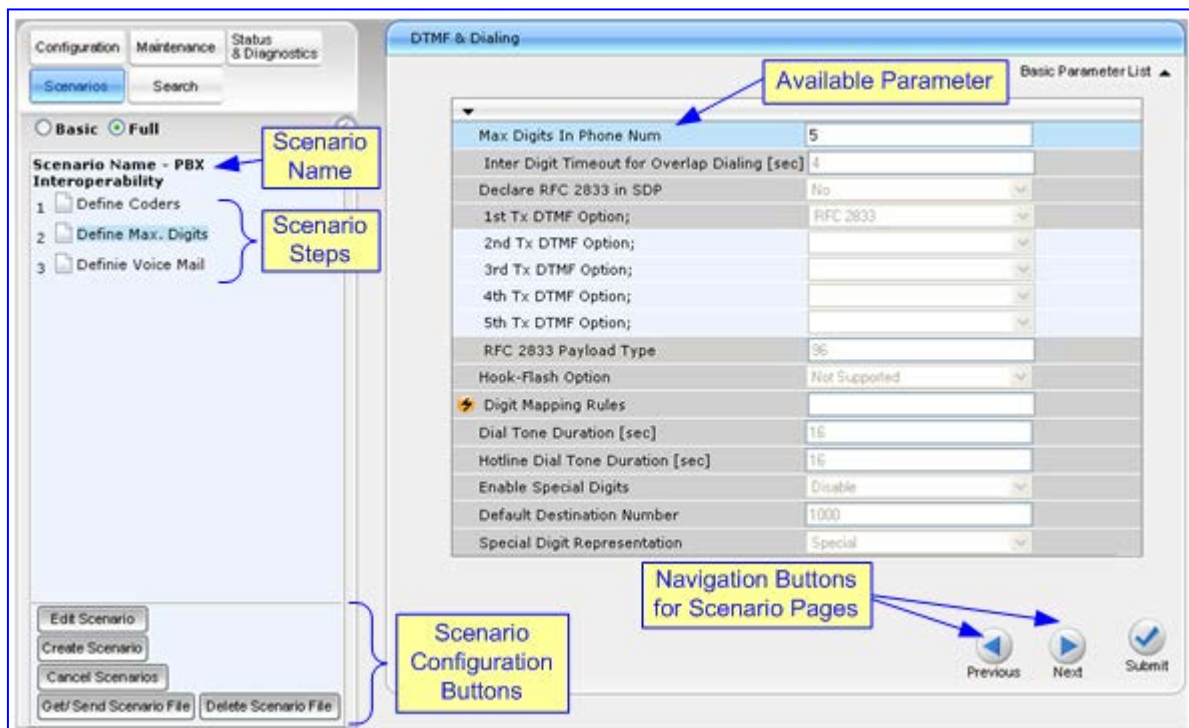
1. On the Navigation bar, select the **Scenario** tab; a message box appears, requesting you to confirm the loading of the Scenario.

Figure 3-21: 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 3-22: 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 the 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 54).

➤ **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 3-23: 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 53).
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 542). The Scenario dat file must be located in the same folder as the ini file. For more information 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:

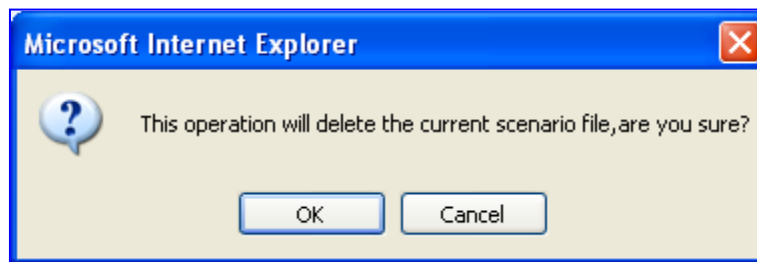
Figure 3-24: Scenario Loading Message Box



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 3-25: 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 54).
- Loading an *ini* file with the ScenarioFileName parameter set to no value (i.e., ScenarioFileName = "").

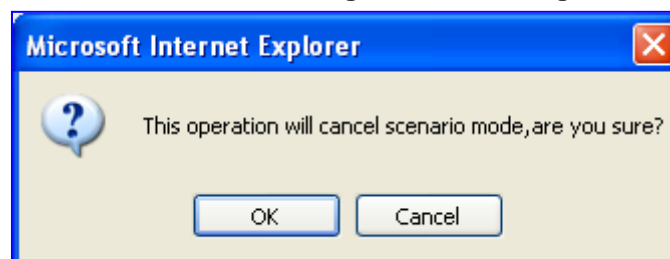
3.1.8.7 Quitting Scenario Mode

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 3-26: 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 Web interface. The *WelcomeMessage* ini file parameter table 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 3-27: User-Defined Web Welcome Message after Login

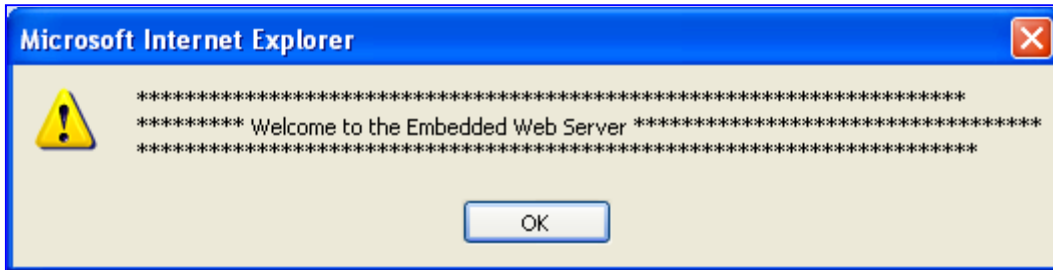


Table 3-2: ini File Parameter for Welcome Login Message

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

3.1.10 Getting Help

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

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


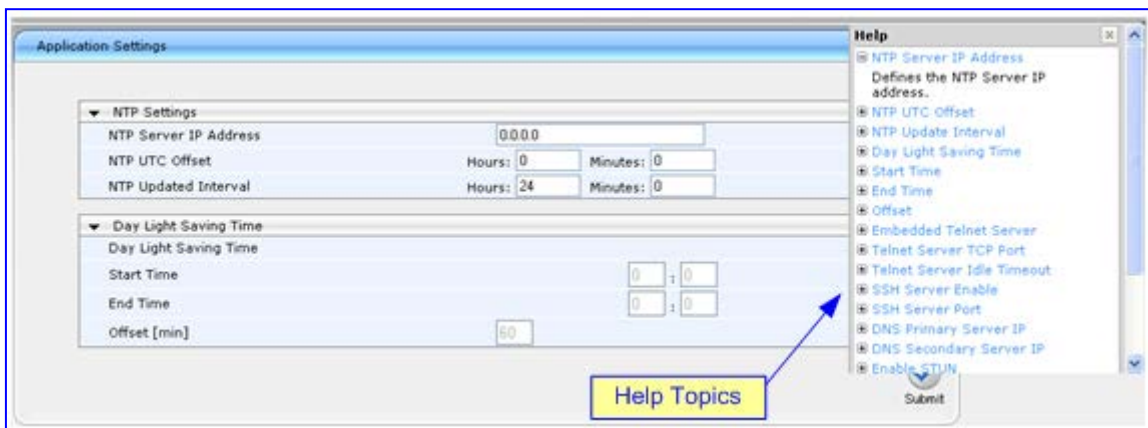




1. On the toolbar, click the **Help**  button; the Help topic pertaining to the opened page appears, as shown below:

Figure 3-28: Help Topic for Current Page



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



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

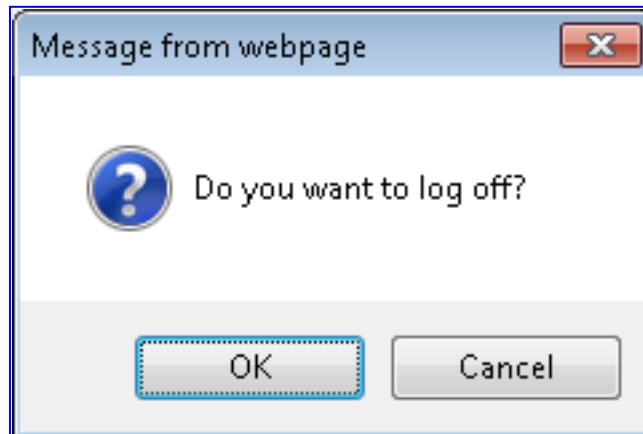
3.1.11 Logging Off the Web Interface

You can log off the Web interface and re-access it with a different user account. For more information on Web User Accounts, see 'Configuring Web User Accounts' on page 66.

➤ **To log off the Web interface:**

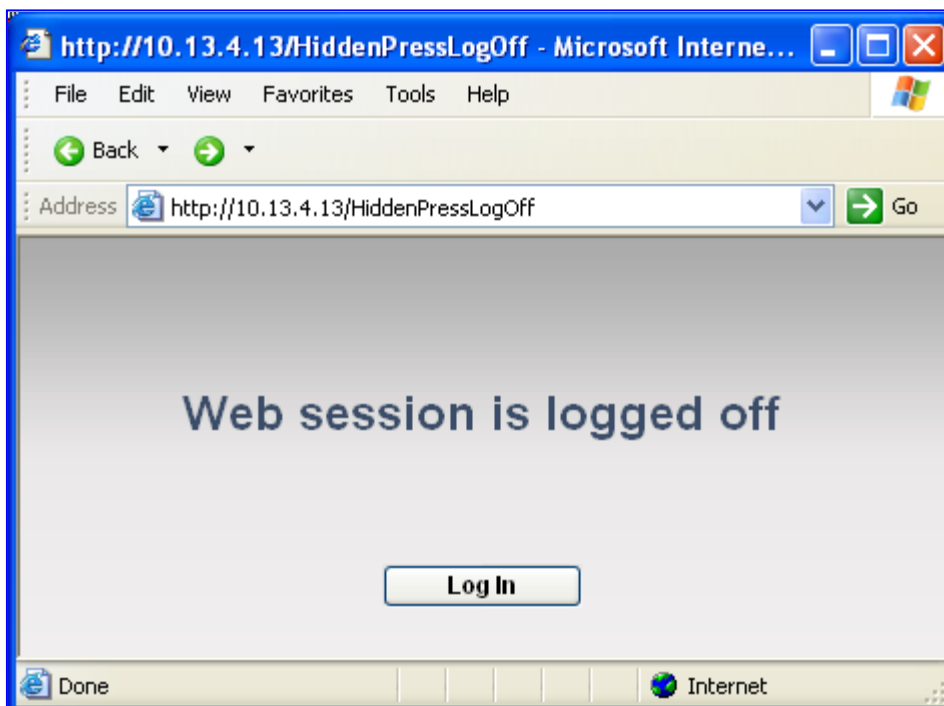
1. On the toolbar, click the **Log Off**  button; the Log Off confirmation message box appears:

Figure 3-29: Log Off Confirmation Box



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

Figure 3-30: Web Session Logged Off



To log in again, simply click the **Log In** button, and then in the Login window, enter your user name and password (see 'Accessing the Web Interface' on page 34).

3.2 Using the Home Page

By default, the Home page is displayed when you access the device's Web interface. The Home page provides you with a graphical display of the device's front panel, 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.

➤ **To access the Home page:**


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

Figure 3-31: Home Page of Mediant 600

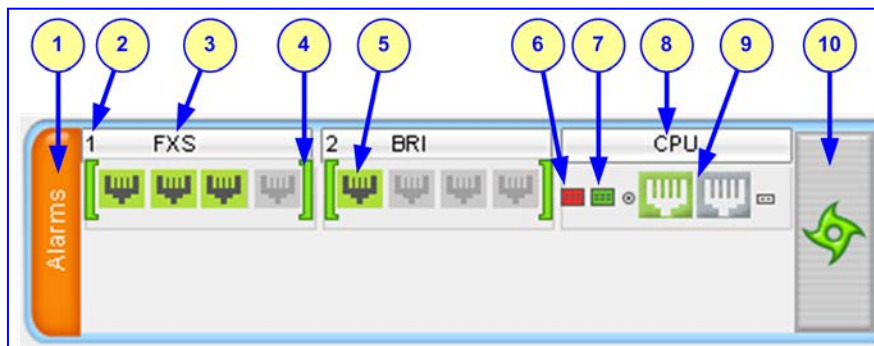
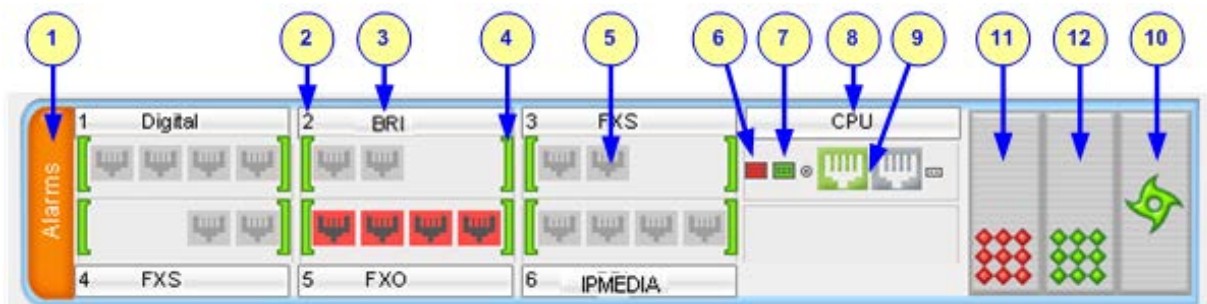


Figure 3-32: Home Page of Mediant 1000



Note: The displayed number and type of telephony interfaces depends on the device's hardware configuration.

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
- **Digital Port Number:** number of digital PRI ports (appears only if the device houses a DIGITAL module)
- **BRI Port Number:** number of BRI ports (appears only if the device houses a BRI module)
- **Analog Port Number:** number of analog (FXS / FXO) ports (appears only if the









device houses any of these analog modules)












- **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 'Basic Maintenance' on page 465.

The table below describes the areas of the Home page.

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

Item #	Description		
1	Displays the highest severity of an active alarm raised (if any) by the device: <ul style="list-style-type: none"> ■ 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 499), click the Alarms area.		
2	Module slot number (1 to 26).		
3	Module type: FXS, FXO, DIGITAL (i.e., E1/T1), BRI, IPMEDIA.		
4	Module status icon: <ul style="list-style-type: none"> ■  (green): Module has been inserted or is correctly configured ■  (gray): Module was removed. 'Reserved' is displayed alongside the module's name ■  (red): Module failure. 'Failure' is displayed instead of the module's name 		
5	Port (trunk or channel) status icon (see Viewing Trunks' Channels on page 63).		
	Icon	Trunk Description (Digital Module)	Channel Description (Analog Module)
	 (grey)	Disable: Trunk not configured (not in use)	Inactive: Channel is currently on-hook
	 (green)	Active - OK: Trunk synchronized	Call Connected: Active RTP stream
	 (yellow)	RAI Alarm: Remote Alarm Indication (RAI), also known as the Yellow Alarm	-
	 (red)	LOS / LOF Alarm: Loss due to LOS (Loss of Signal) or LOF (Loss of Frame)	Not Connected: No analog line is connected to this port or port out of service due to Serial Peripheral Interface (SPI) failure (applicable only to FXO interfaces)
	 (blue)	AIS Alarm: Alarm Indication Signal (AIS), also known as the Blue Alarm	Handset Offhook: Channel is off-hook, but there is no

Item #	Description		
			active RTP session
6	 (orange)	D-Channel Alarm: D-channel alarm	-
7	Dry Contact (normally open) status icon <ul style="list-style-type: none"> ▪  (green): Dry Contact is open (normal) ▪  (red): Dry contact is closed 		
8	Dry Contact (normally closed) status icon: <ul style="list-style-type: none"> ▪  (green): Dry Contact is closed (normal) ▪  (red): Dry contact is open 		
8	CPU module.		
9	Ethernet LAN port status icons: <ul style="list-style-type: none"> ▪  (green): Ethernet link is working ▪  (gray): Ethernet link is not configured You can also view detailed Ethernet port information in the Ethernet Port Information page (see Viewing Ethernet Port Information on page 498), by clicking the icon.		
10	Fan tray unit status icon: <ul style="list-style-type: none"> ▪  (green): Fan tray operating ▪  (red): Fan tray failure 		
11	Power Supply Unit 1 status icon (applicable only to Mediant 1000): <ul style="list-style-type: none"> ▪  (green): Power supply is operating ▪  (red): Power supply failure or no power supply unit installed 		
12	Power Supply Unit 2 status indicator (applicable only to Mediant 1000). See Item #11 for a description.		

3.2.1 Assigning a Port Name

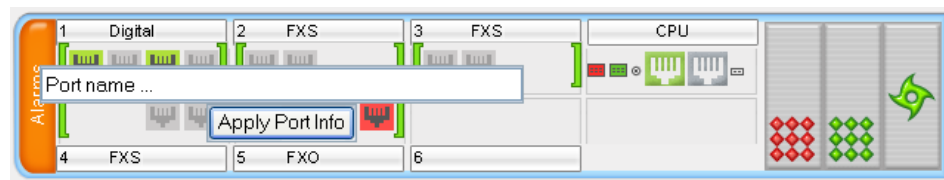
The Home page allows you to assign an arbitrary name or a brief description to each port. This description appears as a tooltip when you move your mouse over the port.

➤ **To add a port description:**

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



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



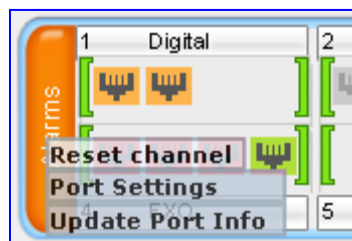
3. Type a brief description for the port, and then click **Apply Port Info**.

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).

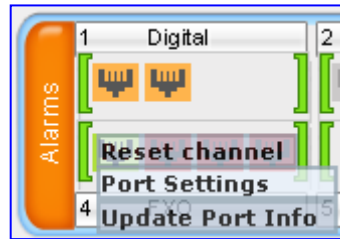


3.2.3 Viewing Analog Port Information

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.



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

Figure 3-33: Basic Information Screen

◆ SIP ◆ Basic ◆ RTP/RTCP ◆ Voice Settings	
Channel Identifier:	6
Status:	Active
Call ID:	0
Endpoint ID:	
Call Duration [sec]:	0
Call Type:	Voice
Call Destination:	0.0.0.0
Coder:	G711Alaw_64

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

3.2.4 Viewing Trunk Channels

The Home page allows you to drill-down to view a detailed status of the channels pertaining to a trunk. In addition, you can view the trunk's configuration.

➤ **To view a detailed status of a trunk's channels:**







- In the Home page, click the trunk port icon of whose status you want to view; a shortcut menu appears.
- From the shortcut menu, choose **Port Settings**; the Trunks & Channels Status page pertaining to the specific trunk appears:

Figure 3-34: Trunks and Channels Status Screen

Trunks	Channels																															
Status	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Trunk 1	[Channel status icons]																															

The color-coding for the status of the trunk's channels status is described in the table below:

Table 3-4: Color-Coding Status for Trunk Channels

Icon	Color	Label	Description
	Light blue	Inactive	Configured, but currently no call
	Green	Active	Call in progress (RTP traffic)
	Purple	SS7	Configured for SS7 Note: Currently, SS7 is not supported.
	Grey	Non Voice	Not configured
	Blue	ISDN Signaling	Configured as a D-channel
	Yellow	CAS Blocked	-

- To view the configuration settings of the trunk and/or to modify the trunk's settings, click the Trunk icon, and then from the shortcut menu, choose Port Settings; the Trunk Settings page appears. For more information on configuring the trunk, see Configuring the Trunk Settings on page 232.

3.2.5 Replacing Modules

To replace the device's modules, you must use the Web interface in combination with physical removal and insertion of the modules. In other words, when you replace a module, you first need to 'software-remove' it, then extract it physically from the chassis and insert a new module, and then 'software-insert' it using the Web interface. The software removal and insertion is performed in the Home page.



Warnings:

- A module must be replaced with the same type of module and in the same module slot number. For example, a module with two digital spans in Slot 1 must be replaced with a module with two digital spans in Slot 1.
- When only one module is available, removal of the module causes the device to reset.
- Before inserting a module into a previously empty slot, you must power down the device.

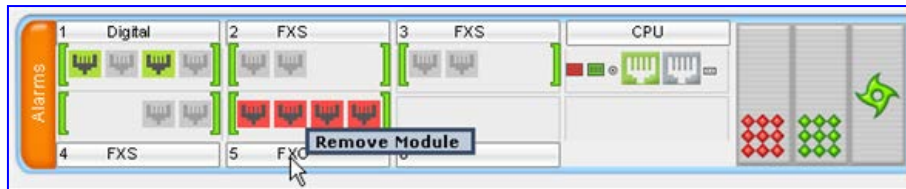


Note: This section is applicable only to Mediant 1000.

➤ **To replace a module:**

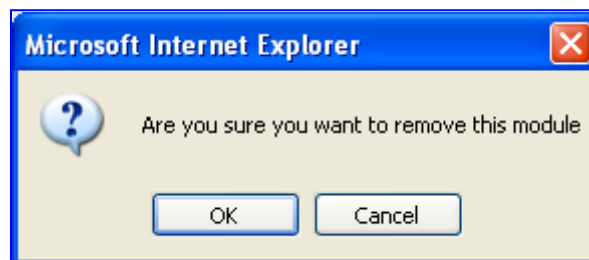
1. Remove the module by performing the following:
 - a. In the Home page, click the title of the module that you want to replace; the **Remove Module** button appears:

Figure 3-35: Remove Module Button

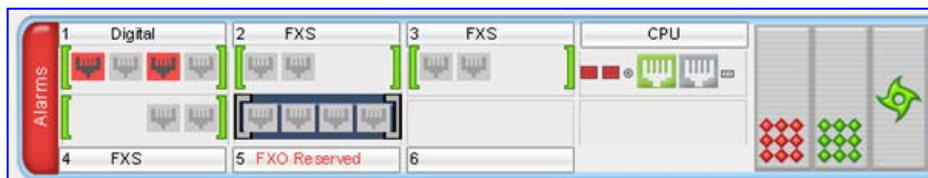


- b. Click the **Remove Module** button; a message box appears requesting you to confirm module removal:

Figure 3-36: Module Removal Confirmation Message Box

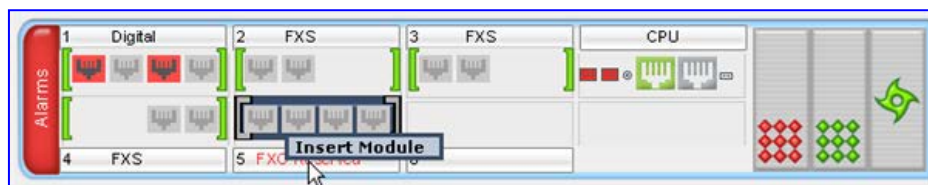


- c. Click **OK** to confirm removal; after a few seconds, the module is software-removed, the module status icon turns to grey, and the name of the module is suffixed with the word 'Reserved':



- d. Physically remove the module (refer to the *Installation Manual*).
2. Insert the replaced module, by performing the following:
 - a. Physically insert the replaced module (refer to the *Installation Manual*) into the same slot in which the previous module resided.
 - b. In the Home page, click the title of the module ("**<module type> Reserved**") that you want to replace; the **Insert Module** button appears:

Figure 3-37: Insert Module Button



- c. Click the **Insert Module** button; a message appears informing you that this may take a few seconds. When the message disappears, the module is inserted, which is indicated by the disappearance of the word 'Reserved' from the module's name.

3.3 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. Users can be banned for a period of time upon a user-defined number of unsuccessful login attempts. Login information (such as how many login attempts were made and the last successful login time) can be presented to the user.

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 3-38: WEB User Accounts Page (for Users with 'Security Administrator' Privileges)

▼ Account Data for User: Admin		
User Name	Admin	<input type="button" value="Change User Name"/>
Access Level	Security Administrat	
▼ Fill in the following 3 fields to change the password		
Current Password	<input type="text"/>	
New Password	<input type="text"/>	
Confirm New Password	<input type="text"/>	<input type="button" value="Change Password"/>
▼ Account Data for User: User		
User Name	User	<input type="button" value="Change User Name"/>
Access Level	User Monitor	<input type="button" value="Change Access Level"/>
▼ Fill in the following 3 fields to change the password		
Current Password	<input type="text"/>	
New Password	<input type="text"/>	
Confirm New Password	<input type="text"/>	<input type="button" value="Change Password"/>
▼ Access Block Parameters		
Deny Authentication Timer	10	
Deny Access On Fail Count	6	
Display Login Information	Yes	

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.



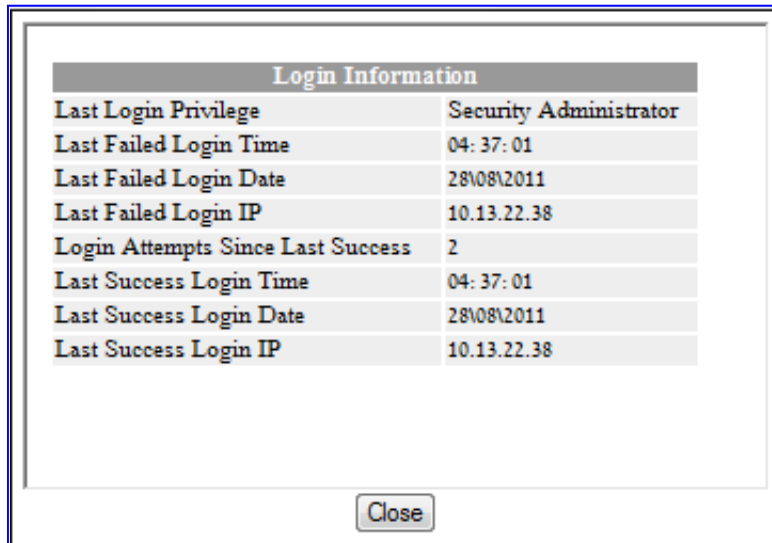
Notes:

- 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.
5. To prevent user access after a specific number of failed logins, do the following:
 - a. From the 'Deny Access On Fail Count' drop-down list, select the number of failed logins after which the user is prevented access to the device for a user-defined time (see next step).
 - b. In the 'Deny Authentication Timer' field, enter the interval (in seconds) that the user needs to wait before a new login attempt from the same IP address can be done after reaching the number of failed login attempts (defined in the previous step).
6. To display user login information upon a successful login, from the 'Display Login Information' drop-down list, select **Yes**. After you login, the following window is displayed:

Figure 3-39: Login Information Window



Login Information	
Last Login Privilege	Security Administrator
Last Failed Login Time	04: 37: 01
Last Failed Login Date	28\08\2011
Last Failed Login IP	10.13.22.38
Login Attempts Since Last Success	2
Last Success Login Time	04: 37: 01
Last Success Login Date	28\08\2011
Last Success Login IP	10.13.22.38

Close

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

**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 542).
- 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*.

3.4 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 542.

➤ **To define Web access security:**

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

HTTP Authentication Mode	Digest When Possible
⚡ Secured Web Connection (HTTPS)	HTTP and HTTPS
Voice Menu Password	12345

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

3.5 Web Login Authentication using Smart Cards

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

This feature is enabled using the EnableMgmtTwoFactorAuthentication parameter.



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

➤ To login to the Web interface using CAC:

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

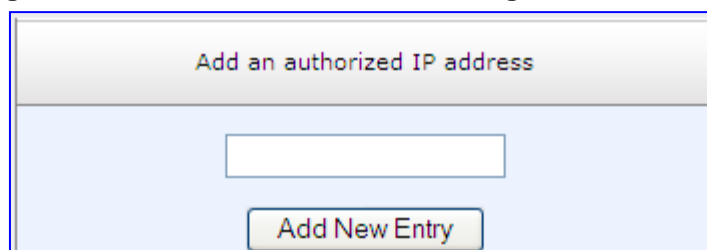
3.6 Configuring Web and Telnet Access List

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 542).

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

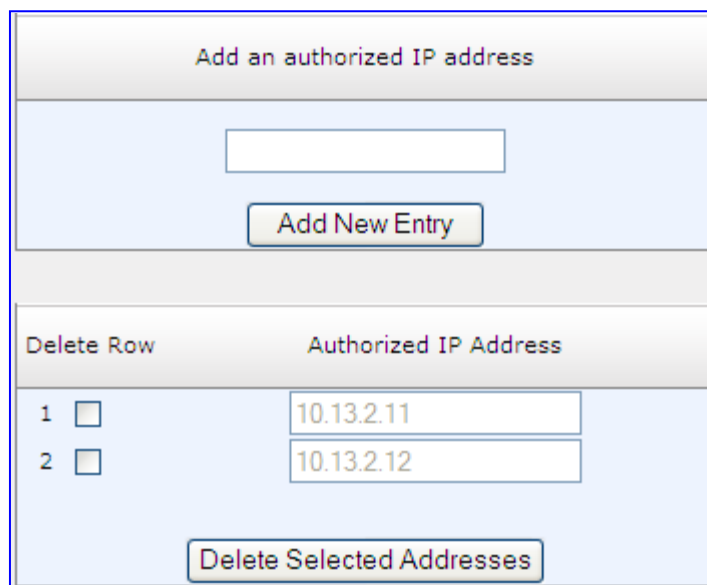
1. Open the Web & Telnet Access List page (**Configuration** tab > **System** menu > **Management** submenu > **Web & Telnet Access List**).

Figure 3-40: Web & Telnet Access List Page - Add New Entry



- 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 3-41: Web & Telnet Access List Table



The screenshot displays a web-based management interface for the Web & Telnet Access List. At the top, there is a section titled "Add an authorized IP address" which contains a text input field and an "Add New Entry" button. Below this is a table with two columns: "Delete Row" and "Authorized IP Address". The table contains two rows of data. The first row has a "1" in the "Delete Row" column, a checkbox, and the IP address "10.13.2.11" in the "Authorized IP Address" column. The second row has a "2" in the "Delete Row" column, a checkbox, and the IP address "10.13.2.12" in the "Authorized IP Address" column. At the bottom of the table, there is a "Delete Selected Addresses" button.

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

- 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.
- To save the changes to flash memory, see 'Saving Configuration' on page 470.



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.

3.7 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 529.

➤ **To configure RADIUS:**

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

Figure 3-42: RADIUS Parameters Page

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

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

4 CLI-Based Management

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

The CLI can be accessed by using the RS-232 serial port or by using SSH or Telnet through the Ethernet interface. Once logged into the CLI with your username and password, you can configure the device by accessing one of the following modes:

- **Basic command mode:** Provides general CLI commands, for example, to display system information and activate debugging. This mode is accessed immediately after you login to the CLI.
- **Enable command mode:** Provides the configuration commands.

To access this mode, type the following:

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

This mode groups the commands under the following command sets:

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



Notes:

- For information on accessing the CLI interface, see 'Using CLI' on page 23.
- For more information on using CLI and for a description of the CLI commands, refer to the books: *MSBG Data CLI Reference Guide* and *MSBG VoIP and System CLI Reference Guide*.

4.1 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 542.

➤ **To define Telnet and SSH:**

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

▼ Telnet Settings		
Embedded Telnet Server	Disable	▼
Telnet Server TCP Port	23	
⚡ Telnet Server Idle Timeout	0	
▼ SSH Settings		
Enable SSH Server	Disable	▼
Server Port	22	
SSH Admin Key		
Require Public Key	Disable	▼
Max Payload Size	32768	
Max Binary Packet Size	35000	
Enable Last Login Message	Enable	▼
Max Login Attempts	3	

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

5 SNMP-Based Management

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

This section provides configuration relating to SNMP management.



Note: For more information on SNMP support, refer to the *Product Reference Manual*.

5.1 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 more information on SNMP community strings, refer to the *Product Reference Manual*. For detailed descriptions of the SNMP parameters, see 'SNMP Parameters' on page 545.

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

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

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

<input type="checkbox"/> Disable SNMP		<input type="text" value="No"/>
Trap Community String		<input type="text" value="trapuser"/>
Trap Manager Host Name		<input type="text"/>

2. Configure the SNMP community strings parameters according to the table below.

3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

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 5-1: SNMP Community String Parameters Description

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

5.2 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 5-1: SNMP Trap Destinations Page

	IP Address	Trap Port	Trap Enable
<input checked="" type="checkbox"/> SNMP Manager 1	10.8.2.28	162	Enable ▾
<input type="checkbox"/> SNMP Manager 2	0.0.0.0	162	Enable ▾
<input type="checkbox"/> SNMP Manager 3	0.0.0.0	162	Enable ▾
<input type="checkbox"/> SNMP Manager 4	0.0.0.0	162	Enable ▾
<input type="checkbox"/> SNMP Manager 5	0.0.0.0	162	Enable ▾

2. Configure the SNMP trap manager parameters according to the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.



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

Table 5-2: 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. <ul style="list-style-type: none"> ▪ [0] (Check box cleared) = Disabled (default) ▪ [1] (Check box selected) = Enabled
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. <ul style="list-style-type: none"> ▪ [0] Disable = Sending is disabled. ▪ [1] Enable = Sending is enabled (default).

5.3 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 5-2: SNMP Trusted Managers

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

2. Select the check box corresponding to the SNMP Trusted Manager that you want to enable and for whom you want to define an IP address.
3. Define an IP address in dotted-decimal notation.
4. Click **Submit** to apply your changes.
5. To save the changes, see 'Saving Configuration' on page 470.

5.4 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 5-3: SNMP V3 Setting Page

Index	User Name	Authentication Protocol	Privacy Protocol	Authentication Key	Privacy Key	Group
1	SueM	MD5	DES	*	*	Read-Write
2	MikeL	None	None	*	*	Trap

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 470.



Notes:

- For a description of the web interface's table command buttons (e.g., **Duplicate** and **Delete**), see 'Working with Tables' on page 44.
- You can also configure SNMP v3 users using the *ini* file table parameter `SNMPUsers` (see 'SNMP Parameters' on page 545).

Table 5-3: SNMP V3 Users Parameters

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

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. <ul style="list-style-type: none">▪ [0] Read-Only (default)▪ [1] Read-Write▪ [2] Trap Note: All groups can be used to send traps.

Reader's Notes

6 EMS-Based Management

AudioCodes Element Management System (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 more information on using the EMS tool, refer to the *EMS User's Manual* and *EMS Server IOM Manual*.

Reader's Notes

7 INI File-Based Management

The *ini* file is a text-based file (created using, for example, Notepad) that can contain any number of parameters settings. The *ini* file can be loaded to the device using the following methods:

- Web interface (see 'Backing Up and Loading Configuration File' on page 491)
- AudioCodes' BootP/TFTP utility (refer to the Product Reference Manual)
- Any standard TFTP server

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

- Using the Load Auxiliary Files page (see 'Loading Auxiliary Files' on page 471): 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 529.
- Some parameters are configurable only through the *ini* file (and not the Web interface).
- To restore the device to default settings using the *ini* file, see 'Restoring Factory Defaults' on page 493.

7.1 INI File Format

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

- Individual parameters (see 'Configuring Individual ini File Parameters' on page 83)
- Table parameters (see 'Configuring ini File Table Parameters' on page 84)

7.1.1 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 example:
[System Parameters]
SyslogServerIP = 10.13.2.69
EnableSyslog = 1
; these are a few of the system-related parameters.
```

For general *ini* file formatting rules, see 'General ini File Formatting Rules' on page 85.

7.1.2 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 85.

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 ]
```



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.

7.1.3 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.

7.2 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 491).
2. Open the *ini* file (using a text file editor such as 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 491).



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

7.3 Secured Encoded ini File

The *ini* file contains sensitive information that is required for the functioning of the device. The file may be loaded to the device using 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 Loading Configuration File' on page 491).
- 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).



Part III

General System Settings

This part provides general system configurations.

Reader's Notes

8 Configuring Certificates

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

- Replace the device's certificate - see 'Replacing Device Certificate' on page 89
- Load a new private key from an external source - see 'Loading a Private Key' on page 92
- Configure trusted root certificates - see 'Mutual TLS Authentication' on page 93
- Regenerate keys and self-signed certificates - see 'Self-Signed Certificates' on page 94



Note: The device is shipped with a working TLS configuration. Therefore, configure certificates only if required.

8.1 Replacing Device Certificate

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

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

1. Your network administrator should allocate a unique DNS name for the device (e.g., dns_name.corp.customer.com). This DNS name is used to access the device and therefore, must be listed in the server certificate.
2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' field (HTTPSOOnly) to **HTTP and HTTPS** (see 'Configuring Web Security Settings' on page 69). This ensures that you have a method for accessing the device in case the new certificate does not work. Restore the previous setting after testing the configuration.

- Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**).

Figure 8-1: Certificates Page

▼ Certificate information

Certificate subject:	/CN=ACL_3845462
Certificate issuer:	/CN=ACL_3845462
Time to expiration:	3041 days
Key size:	1024 bits
Private key:	OK

▼ Certificate Signing Request

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

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

▼ Generate new private key and self-signed certificate

Private Key Size	1024
------------------	------

Press the button "Generate self-signed" to create a self-signed certificate using the subject name provided above.
Important: this is a lengthy operation, during this time the device will be out of service.
 After the operation is complete, save configuration and reset the device.

▼ Upload certificate files from your computer

Private key pass-phrase <i>(optional)</i>	audc
---	------

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

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

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

Send **"Trusted Root Certificate Store"** file from your computer to the device.
 The file must be in textual PEM format.

4. Under the **Certificate Signing Request** group, do the following:
 - a. In the 'Subject Name [CN]' field, enter the DNS name.
 - b. Fill in the rest of the request fields according to your security provider's instructions.
 - c. Click **Create CSR**; a textual certificate signing request is displayed.
5. Copy the text and send it to your security provider. The security provider (also known as Certification Authority or CA) signs this request and then sends you a server certificate for the device.
6. Save the certificate to a file (e.g., cert.txt). Ensure that the file is a plain-text file containing the 'BEGIN CERTIFICATE' header, as shown in the example of a Base64-Encoded X.509 Certificate below:

```
-----BEGIN CERTIFICATE-----
MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJGUj
ETMBEGA1UEChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBTZXJ2ZXVy
MB4XDTk4MDYyNDA4MDAwMFoXDTE4MDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRlIxEz
ARBgNVBAoTCKNlcnRpcG9zdGUXGzAZBgNVBAMTEkNlcnRpcG9zdGUGU2VydmlvIjCC
ASEwDQYJKoZIhvcNAQEBBQADggEAOADCCAQkCggEAPqd4MziR4spWldGRx8bQrhZkon
WnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7
JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRefiXDmuOe+FhJ
gHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuZDIUPlF1jMa+LPwvREXfFcUW+w==
-----END CERTIFICATE-----
```

7. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the cert.txt file, and then click **Send File**.
8. After the certificate successfully loads to the device, save the configuration with a device reset (see 'Saving Configuration' on page 470); the Web interface uses the provided certificate.
9. Open the Certificates page again and verify that under the **Certificate information** group (at the top of the page), the 'Private key' read-only field displays "OK"; otherwise, consult your security administrator.
10. If the device was originally operating in HTTPS mode and you disabled it in Step 2, then return it to HTTPS by setting the 'Secured Web Connection (HTTPS)' field to **HTTPS Only**.


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 device certificate can also be loaded via the Automatic Update Facility, using the HTTPSCertFileName *ini* file parameter.

8.2 Loading a Private Key

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

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

1. Your security administrator should provide you with a private key in either textual PEM (PKCS #7) or PFX (PKCS #12) format. The file may be encrypted with a short pass-phrase, which should be provided by your security administrator.
2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' field (HTTPSONly) to **HTTP and HTTPS** (see 'Configuring Web Security Settings' on page 69). This ensures that you have a method for accessing the device in case the new configuration does not work. Restore the previous setting after testing the configuration.
3. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**) and scroll down to the **Upload certificate files from your computer** group.
4. Fill in the 'Private key pass-phrase' field, if required.
5. Click the **Browse** button corresponding to the 'Send Private Key' field, navigate to the key file, and then click **Send File**.
6. If the security administrator has provided you with a device certificate file, load it using the 'Send Device Certificate' field.
7. After the files successfully load to the device, save the configuration with a device reset (see 'Saving Configuration' on page 470); the Web interface uses the new configuration.
8. Open the Certificates page again, and verify that under the **Certificate information** group (at the top of the page) the 'Private key' read-only field displays "OK"; otherwise, consult your security administrator.
9. If the device was originally operating in HTTPS mode and you disabled it in Step 2, then enable it by setting the 'Secured Web Connection (HTTPS)' field to **HTTPS Only**.

8.3 Mutual TLS Authentication

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

Since X.509 certificates have an expiration date and time, the device must be configured to use NTP (see 'Simple Network Time Protocol Support' on page 95) to obtain the current date and time. Without the correct date and time, client certificates cannot work.

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

1. Set the 'Secured Web Connection (HTTPS)' field to **HTTPS Only** (see 'Configuring Web Security Settings' on page 69) to ensure you have a method for accessing the device in case the client certificate does not work. Restore the previous setting after testing the configuration.
2. Open the Certificates page (see 'Replacing Device Certificate' on page 89).
3. In the **Upload certificate files from your computer** group, click the **Browse** button corresponding to the 'Send Trusted Root Certificate Store ...' field, navigate to the file, and then click **Send File**.
4. When the operation is complete, set the 'Requires Client Certificates for HTTPS connection' field to **Enable** (see 'Configuring Web Security Settings' on page 69).
5. Save the configuration with a device reset (see 'Saving Configuration' on page 470).

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

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



Notes:

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

8.4 Self-Signed Certificates

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

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

1. Before you begin, ensure the following:
 - You have a unique DNS name for the device (e.g., `dns_name.corp.customer.com`). This name is used to access the device and should therefore, be listed in the server certificate.
 - No traffic is running on the device. The certificate generation process is disruptive to traffic and should be executed during maintenance time.
2. Open the Certificates page (see 'Replacing Device Certificate' on page [89](#)).
3. In the 'Subject Name [CN]' field, enter the fully-qualified DNS name (FQDN) as the certificate subject, select the desired private key size (in bits), and then click **Generate self-signed**; after a few seconds, a message appears displaying the new subject name.
4. Save the configuration with a device reset (see 'Saving Configuration' on page [470](#)) for the new certificate to take effect.

9 Date and Time

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

9.1 Configuring Manual Date and Time

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

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 9-1: Regional Settings Page

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

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 Simple Network Time Protocol Support (SNTP) server, the fields on this page display the received date and time and are read-only.
- After performing a hardware reset, the date and time are returned to their defaults and therefore, should be updated.

9.2 Configuring Automatic Date and Time through SNTP Server

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

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

The client requests a time update from a specified NTP server at a specified update interval. In most situations, this update interval is every 24 hours based on when the system was restarted. The NTP server identity (as an IP address) 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.

The procedure below describes how to configure SNTP using the Web interface.

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

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

▼ NTP Settings			
NTP Server IP Address	<input type="text" value="0.0.0.0"/>		
NTP UTC Offset	Hours: <input type="text" value="0"/>	Minutes: <input type="text" value="0"/>	
NTP Updated Interval	Hours: <input type="text" value="24"/>	Minutes: <input type="text" value="0"/>	
▼ Day Light Saving Time			
Day Light Saving Time	<input type="text" value="Disable"/>		
Start Time	<input type="text" value="Jan"/>	<input type="text" value="01"/>	<input type="text" value="00"/>
End Time	<input type="text" value="Jan"/>	<input type="text" value="01"/>	<input type="text" value="00"/>
Offset [min]	<input type="text" value="60"/>		
▼ STUN Settings			
⚡ Enable STUN	<input type="text" value="Disable"/>		
⚡ STUN Server Primary IP	<input type="text" value="0.0.0.0"/>		
⚡ STUN Server Secondary IP	<input type="text" value="0.0.0.0"/>		
▼ NFS Settings			
NFS Table			
▼ DHCP Settings			
Enable DHCP	<input type="text" value="Disable"/>		

2. Configure the NTP parameters:
 - 'NTP Server IP Address' (NTPServerIP) - defines the IP address of the NTP server
 - 'NTP UTC Offset' (NTPServerUTCOffset) - defines the time offset in relation to the UTC. For example, if your region is 2 hours ahead of the UTC, enter "2".
 - 'NTP Updated Interval' (NTPUpdateInterval) - defines the period after which the date and time of the device is updated

3. Configure daylight saving, if required:
 - 'Day Light Saving Time' (DayLightSavingTimeEnable) - enables daylight saving time
 - 'Start Time' (DayLightSavingTimeStart) and 'End Time' (DayLightSavingTimeEnd) - defines the period for which daylight saving time is relevant.
 - 'Offset' (DayLightSavingTimeOffset) - defines the offset in minutes to add to the time for daylight saving. For example, if your region has daylight saving of one hour, the time received from the NTP server is 11:00, and the UTC offset for your region is +2 (i.e., 13:00), you need to enter "60" to change the local time to 14:00.
4. Verify that the device is set to the correct date and time. You can do this by viewing the date and time in the Regional Settings page, as described in 'Configuring Date and Time' on page 95.

Reader's Notes



Part IV

VoIP Configuration

This part describes the VoIP configurations.

Reader's Notes

10 Network

This section describes the network-related configuration.

10.1 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 Half-Duplex or 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.

10.2 Ethernet Interface Redundancy

The device supports Ethernet redundancy by providing two Ethernet ports, located on the CPU module. The Ethernet port redundancy feature is enabled using the ini file parameter `MIIRedundancyEnable`. By default, this feature is disabled.

When Ethernet redundancy is implemented, the two Ethernet ports can be connected to the same switch (segment / hub). In this setup, one Ethernet port is active and the other is redundant. If an Ethernet connection failure is detected, the CPU module switches over to the redundant Ethernet port. The CPU issues a Major alarm notifying of the failed physical port. If the first Ethernet port connection is restored, the Major alarm is cleared. The first physical port now becomes the redundant Ethernet port in case of failure with the active physical port (which is currently the second physical port).

When the CPU module loses all Ethernet connectivity, a Critical alarm is generated:

- When `MIIRedundancyEnable` is disabled: the alarm is generated when the single physical connection is lost. The alarm is cleared when the single physical connection is restored.
- When `MIIRedundancyEnable` is enabled: the alarm is generated when both physical connections are lost. The alarm is cleared when one or both of the physical connections are restored.

10.3 Configuring IP Interface Settings

The Multiple Interface Table page allows you to configure logical VoIP network interfaces. Each interface can be defined with the following:

- Application type allowed on the interface:
 - Control - call control signaling traffic (i.e., SIP)
 - Media - RTP traffic
 - Operations, Administration, Maintenance and Provisioning (OAMP) - management (such as Web- and SNMP-based management)
- IP address and subnet
- VLAN ID
- Default Gateway
- Primary and secondary DNS IP address

You can configure up to 16 interfaces - up to 15 Control and/or Media interfaces, and 1 OAMP interface.

This page also provides VLAN-related parameters for enabling VLANs and defining the Native VLAN ID. This is the 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 122](#).

**Notes:**

- For more information and examples of network interfaces configuration, see 'Network Configuration' on page 106.
- 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 Firewall Settings' on page 131).
- You can view currently active configured IP interfaces in the 'IP Active Interfaces' page (see 'Viewing Active IP Interfaces' on page 505).
- You can also configure this table using the *ini* file table parameter InterfaceTable (see 'Networking Parameters' on page 531).
- For configuring Web interface tables, see 'Working with Tables' on page 44.

➤ **To configure IP network interfaces:**

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

Figure 10-1: IP Settings Page

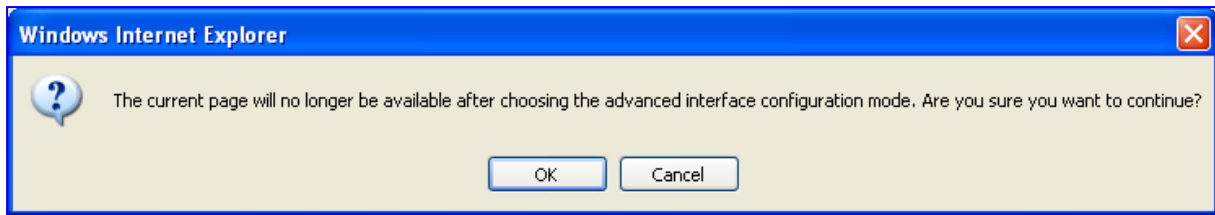
Single IP Settings	
IP Address	<input type="text" value="10.33.4.35"/>
Subnet Mask	<input type="text" value="255.255.0.0"/>
Default Gateway Address	<input type="text" value="10.33.0.1"/>
▼ VoIP DNS Settings	
⚡ DNS Primary Server IP	<input type="text"/>
⚡ DNS Secondary Server IP	<input type="text"/>
▼ Multiple Interface Settings	
Multiple Interface Table	<input type="button" value="➡"/>



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.

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

Figure 10-2: Confirmation Message for Accessing the Multiple Interface Table



- Click OK to confirm; the 'Multiple Interface Table' page appears:

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP + Media + Control	10.13.4.13	16	10.13.0.1	1	O+M+C

VLAN Mode Enable
 Native VLAN ID 1
 IP Interface Status Table

- 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.
- Configure the interface according to the table below.
- Click the **Apply** button; the interface is added to the table and the **Done** button appears.
- 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 112), a warning message is displayed.
- Save the changes to flash memory and reset the device (see 'Saving Configuration' on page 470).

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 505.

Table 10-1: Multiple Interface Table Parameters Description

Parameter	Description
Table parameters	
Index	Table index row of the interface. The range is 0 to 15.
Web: Application Type EMS: Application Types [InterfaceTable_ApplicationTypes]	Defines the types of applications allowed on the interface. <ul style="list-style-type: none"> ▪ [0] OAMP = Operations, Administration, Maintenance and Provisioning (OAMP) applications (e.g., Web, Telnet, SSH, and SNMP). ▪ [1] Media = Media (i.e., RTP streams of voice). ▪ [2] Control = Call Control applications (e.g., SIP). ▪ [3] OAMP + Media = OAMP and Media applications. ▪ [4] OAMP + Control = OAMP and Call Control applications.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [5] Media + Control = Media and Call Control applications. ▪ [6] OAMP + Media + Control = All application types are allowed on the interface. <p>Note: For valid configuration guidelines, see 'Multiple Interface Table Configuration Summary and Guidelines' on page 112.</p>
Web/EMS: IP Address [InterfaceTable_IPAddress]	<p>The IPv4 IP address in dotted-decimal notation.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>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).</p> <p>The prefix length is a Classless Inter-Domain Routing (CIDR) style presentation of a dotted-decimal subnet notation. The CIDR-style presentation is the latest method for interpretation of IP addresses. Specifically, instead of using eight-bit address 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).</p> <p>For IPv4 Interfaces, the prefix length values range from 0 to 31.</p> <p>Note: Subnets of different interfaces must not overlap in any 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.</p>
Web/EMS: Gateway [InterfaceTable_Gateway]	<p>Defines the IP address of the default gateway for this interface.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.

Parameter	Description
Web/EMS: VLAN ID [InterfaceTable_VlanID]	<p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> 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]	<p>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 Media Realm table and SIP Interface table.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is mandatory. The name must be unique for each interface.
Web/EMS: Primary DNS Server IP address [InterfaceTable_PrimaryDNSServerIPAddress]	<p>Defines the IP address (in dotted-decimal notation) of the primary DNS server that is used for translating domain names into IP addresses for each interface.</p> <p>Note: This parameter is optional.</p>
Web/EMS: Secondary DNS Server IP address [InterfaceTable_SecondaryDNSServerIPAddress]	<p>Defines the IP address (in dotted-decimal notation) of the secondary DNS server that is used for translating domain names into IP addresses for each interface.</p> <p>Note: This parameter is optional.</p>
General Parameters	
VLAN Mode [VLANMode]	For a description of this parameter, see Networking Parameters on page 531.
Native VLAN ID [VLANNativeVlanID]	For a description of this parameter, see Networking Parameters on page 531.

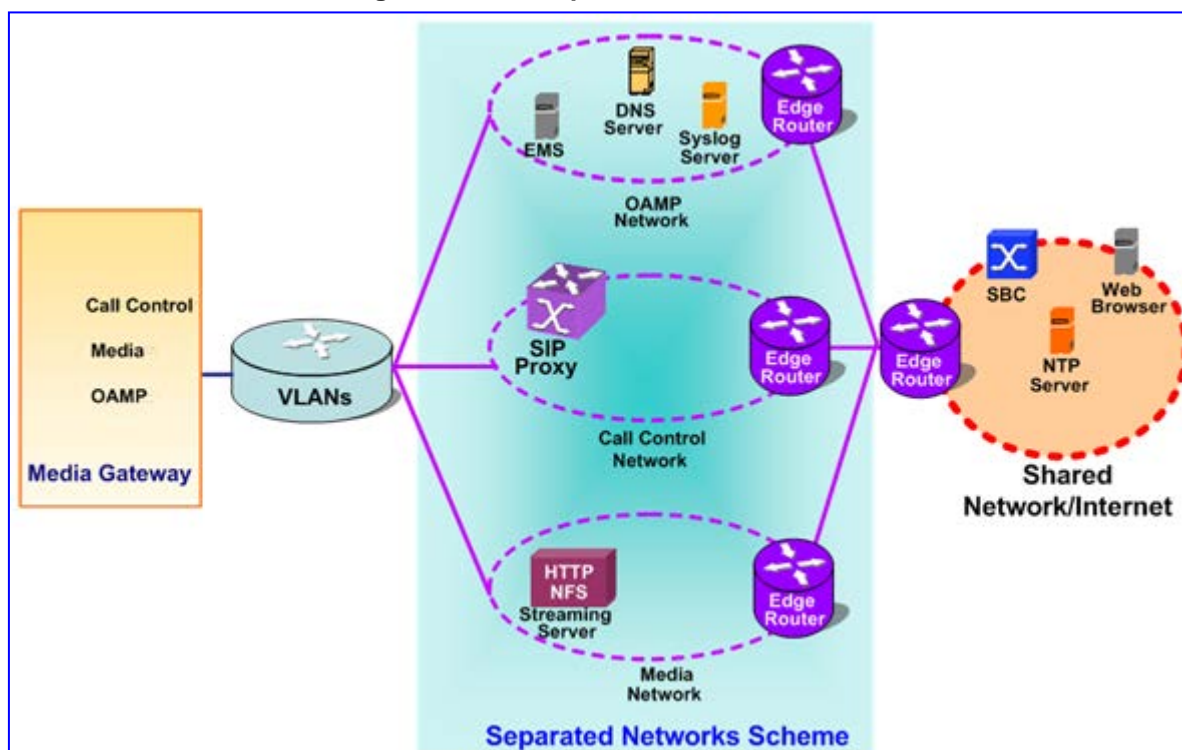
10.3.1 Network Configuration

The device allows you to configure multiple 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.

10.3.1.1 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 10-3: 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 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.

10.3.1.1.1 Overview of Multiple Interface Table

The Multiple Interfaces scheme allows you to define different IP addresses and VLANs in a table format, as shown below:

Table 10-2: 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

Index Mode	Application	Interface	IP Address	Prefix Length	Default Gateway	VLAN ID	Interface Name
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 111).

10.3.1.1.2 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 109 for more details.

10.3.1.1.2.1 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.

10.3.1.1.2.2 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 'Configuring the IP Routing Table' on page 118 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 10-3: Configured Default Gateway Example

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP	IPv4 Manual	192.168.085.214	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 enables OAMP applications to access peers on subnet 17.17.0.0 through the gateway 192.168.0.1.

Table 10-4: Separate Routing Table Example

Destination	Prefix Length	Gateway	Interface	Metric	Status
17.17.0.0	16	192.168.0.1	0	1	Active

10.3.1.1.2.3 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.

10.3.1.1.2.4 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.

10.3.1.1.2.5 Primary / Secondary DNS Server IP Address Columns

Defines the primary and secondary DNS server IP addresses for translating domain names into IP addresses.

10.3.1.1.3 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.

10.3.1.1.3.1 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.

10.3.1.1.3.2 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).

10.3.1.1.3.3 '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.

10.3.1.1.3.4 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.

For Layer-3 CoS, you can use the PremiumServiceClassMediaDiffServ, PremiumServiceClassControlDiffServ, GoldServiceClassDiffServ, and BronzeServiceClassDiffServ parameters.

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

Table 10-5: 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: <ul style="list-style-type: none"> ▪ OAMP ▪ Control 	Depends on traffic type: <ul style="list-style-type: none"> ▪ Control: Premium Control ▪ Management: Bronze
NTP	Varies according to NTP settings	Depends on traffic type:

Application	Traffic / Network Types	Class-of-Service (Priority)
	(EnableNTPasOAM): <ul style="list-style-type: none"> ▪ OAMP ▪ Control 	<ul style="list-style-type: none"> ▪ Control: Premium control ▪ Management: Bronze
NFS	NFSServers_VlanType in the NFSServers table	Gold

10.3.1.1.3.5 Assigning NTP Services to Application Types

NTP applications can be associated with different application types (OAMP or Control) in different setups. The table below describes the parameter for configuring this:

Table 10-6: Application Type Parameters

Parameter	Description
EnableNTPasOAM	Determines the application type for NTP services. <ul style="list-style-type: none"> ▪ [1] = OAMP (default) ▪ [0] = Control. Note: For this parameter to take effect, a device reset is required.

10.3.1.1.4 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 OAMP interface must be configured, and this must be of address type IPv4. This OAMP interface can be combined with Media and Control interfaces.
- At least one IPv4 interface with CONTROL "Application Types" **must** be configured.
- At least one IPv4 interface with MEDIA "Application Types" **must** be configured.
- The application types **may** be mixed, for example:
 - 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 ('Configuring the IP Routing Table' on page 118).

- 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.
- Primary and Secondary DNS server address may be configured for each interface. **Note:** Currently, the device supports DNS configuration for only one interface.
- 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. Ensure that you view 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.

10.3.1.1.5 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, 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.

10.3.1.2 Setting Up VoIP Networking

10.3.1.2.1 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 NTP applications:
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_PrimaryDNSServerIPAddress, InterfaceTable_SecondaryDNSServerIPAddress;
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 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.

10.3.1.2 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 10-7: 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 10-8: 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 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_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress;
```

```

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 10-9: Multiple Interface Table - Example 2

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 10-10: 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 NTP application remains with its 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_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress;
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 Interfaces: one exclusively for management (OAMP applications) and two others for Call Control and RTP (Control and Media applications) :

Table 10-11: 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 10-12: 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 NTP application remains with its 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_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress;
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 ]
    
```

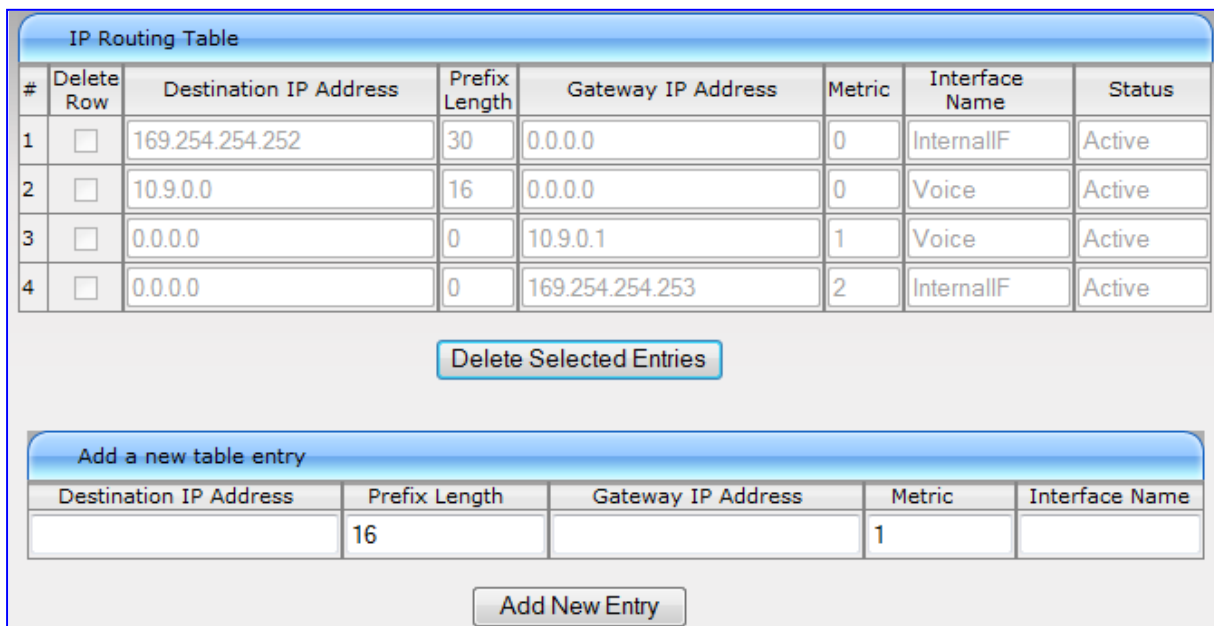
10.4 Configuring the IP Routing Table

The IP Routing Table page allows you to define up to 30 static IP routing rules for the device. These rules can be associated with a network interface (defined in the Multiple Interface table) and therefore, the routing decision is based on the source subnet/VLAN. If not associated with an IP interface, the static IP rule is based on destination IP address. 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 102).

➤ **To configure static IP routing:**

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

Figure 10-4: IP Routing Table Page



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

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

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 10-13: 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.
<p>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.</p> <p>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'.</p>	
Gateway IP Address [StaticRouteTable_Gateway]	<p>The IP address of the router (next hop) to which the packets are sent if their destination matches the rules in the adjacent columns.</p> <p>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.</p>
Metric	<p>The number of hops needed to get to the specified destination.</p> <p>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.</p>
Interface Name [StaticRouteTable_InterfaceName]	<p>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 102).</p> <p>Note: The IP address of the 'Gateway IP Address' field must be in the same subnet as this interface's IP address.</p>
Status	<p>Read-only field displaying the status of the static IP route:</p> <ul style="list-style-type: none"> ▪ "Active" - routing rule is used by the device ▪ "Inactive" - routing rule is not applied

10.4.1 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.

The IP Routing table consists of the following:

Table 10-14: 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

10.4.1.1 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.

10.4.1.2 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.

10.4.1.3 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.

10.4.1.4 Interface Column

This column defines the interface index (in the Multiple Interface table) from which the gateway address is reached.

Figure 10-5: Interface Column

The Interface Table:

Index	Allowed Application Types	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	0	10	10.31.174.50	16	0.0.0.0	4	ManagementIF
1	2	10	10.32.174.50	16	0.0.0.0	5	ControlIF
2	1	10	10.33.174.50	16	10.33.0.1	6	Media1IF
3	1	10	10.34.174.50	16	0.0.0.0	7	Media2IF
4	5	4	2000::1:10:33:174:50	64	::	6	V6MedCtrl

The Routing Table:

Destination	Prefix Length	Subnet Mask	Gateway	Interface	Hop Count
201.201.0.0	16	...	10.31.174.1	0	1
		...			

Left Blank

The Gateway address resides on the subnet configured in Interface Index 0 at the Interface Table. The Next Hop will be accessible via Interface 0.

10.4.1.5 Metric Column

The Metric column must be set to 1 for each static routing rule.

10.4.1.6 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".

10.4.2 Routing Table Configuration Summary and Guidelines

The Routing table configurations must adhere to the following rules:

- Up to 30 different static routing rules 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.

10.4.3 Troubleshooting the Routing Table

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

Common routing rule configuration errors may include the following:

- The IP address specified in the "Gateway" 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.

10.5 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 531. For a description on QoS and the mapping of each application to a class of service, see 'Quality of Service Parameters' on page 111.

➤ **To configure QoS:**

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

▼ Priority Settings	
Network Priority	<input type="text" value="7"/>
Media Premium Priority	<input type="text" value="6"/>
Control Premium Priority	<input type="text" value="6"/>
Gold Priority	<input type="text" value="4"/>
Bronze Priority	<input type="text" value="2"/>
▼ Differential Services	
Network QoS	<input type="text" value="48"/>
Media Premium QoS	<input type="text" value="46"/>
Control Premium QoS	<input type="text" value="40"/>
Gold QoS	<input type="text" value="26"/>
Bronze QoS	<input type="text" value="10"/>

2. Configure the QoS parameters as required.
3. Click **Submit** to apply your changes.
4. Save the changes to flash memory (see 'Saving Configuration' on page 470).

10.6 DNS

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

The device supports the configuration of the following DNS types:

- Internal DNS table - see 'Configuring the Internal DNS Table' on page 123
- Internal SRV table - see 'Configuring the Internal SRV Table' on page 124

10.6.1 Configuring the Internal DNS Table

The Internal DNS Table page, similar to a DNS resolution translates up to 20 host (domain) names into IP addresses (e.g., when using the Outbound IP Routing Table 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 the Multiple Interface table - see 'Configuring IP Interface Settings' on page 102).
- You can also configure the DNS table using the *ini* file table parameter DNS2IP (see 'DNS Parameters' on page 539).

➤ **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 10-6: Internal DNS Table Page

Internal DNS Index					
	Domain Name	First IP Address	Second IP Address	Third IP Address	Fourth IP Address
1	domainname.com	10.8.2.15	10.8.4.20	10.8.16.17	10.8.16.18
2					
3					
4					
5					
6					
7					
8					
9					
10					

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 **Submit** to apply your changes.
6. To save the changes to flash memory, see 'Saving Configuration' on page 470.

10.6.2 Configuring the Internal SRV Table

The Internal SRV Table page resolves host names to DNS A-Records. Three different A-Records can be assigned to each host name. 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 the Multiple Interface table - see 'Configuring IP Interface Settings' on page 102).
- You can also configure the Internal SRV table using the *ini* file table parameter SRV2IP (see 'DNS Parameters' on page 539).

➤ **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 10-7: Internal SRV Table Page

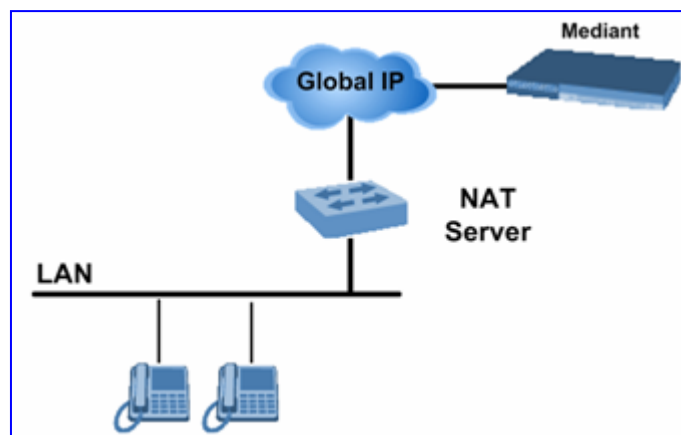
	Domain Name	Transport Type	DNS Name 1	Priority	Weight	Port	DNS Name 2	Priority	Weight	Port	DNS Name 3	Priority	Weight	Port
1		UDP												
2		UDP												
3		UDP												
4		UDP												
5		UDP												
6		UDP												
7		UDP												
8		UDP												
9		UDP												
10		UDP												

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 **Submit** to apply your changes.
9. To save the changes so they are available after a hardware reset or power fail, see 'Saving Configuration' on page 470.

10.7 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.



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 126)
- First Incoming Packet Mechanism (see 'First Incoming Packet Mechanism' on page 127)
- RTP No-Op packets according to the avt-rtp-noop draft (see 'No-Op Packets' on page 127)

For information on SNMP NAT traversal, refer to the *Product Reference Manual*.

10.7.1 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.

10.7.2 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.

10.7.3 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 531.

- **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 531). 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.

10.8 Configuring NFS Settings

Network File System (NFS) enables the device to access a remote server's shared files and directories, and to handle them as if they're located locally. 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.


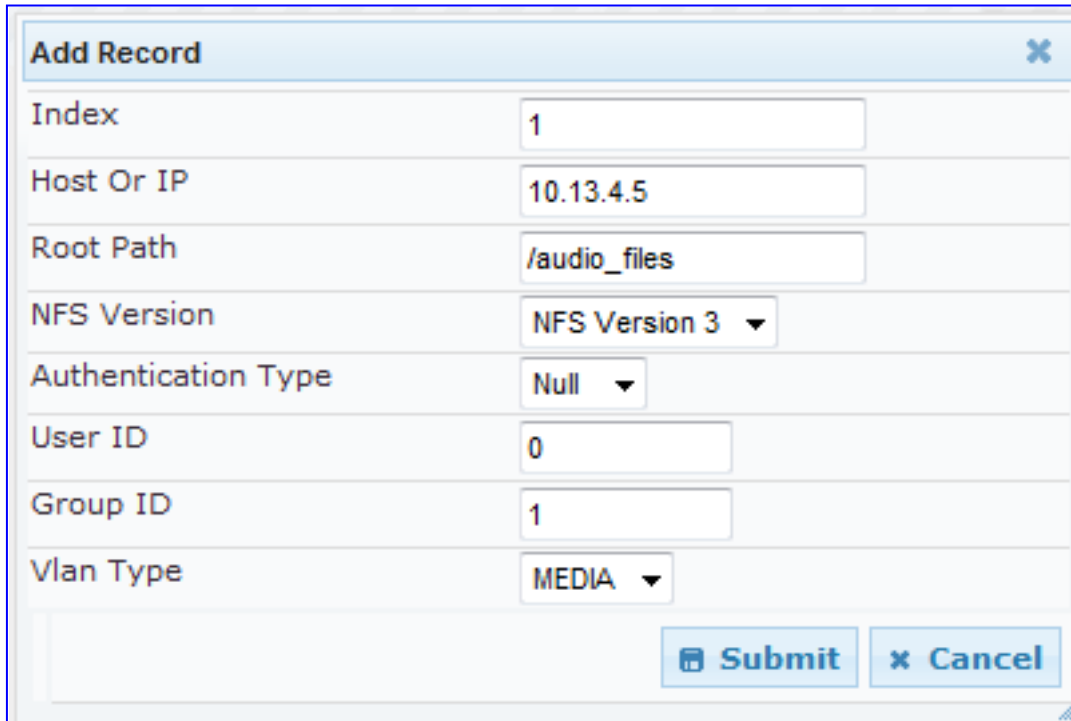
- **To add remote NFS file systems:**
- 1. Open the Application Settings page (**Configuration** tab > **System** menu > **Application Settings**).
- 2. Under the NFS Settings group, click the **NFS Table**  button; the NFS Settings page appears.
- 3. Click the **Add** button; the Add Record dialog box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

Figure 10-8: Add Record Dialog Box for NFS



Index	1
Host Or IP	10.13.4.5
Root Path	/audio_files
NFS Version	NFS Version 3
Authentication Type	Null
User ID	0
Group ID	1
Vlan Type	MEDIA

- 4. Configure the NFS parameters according to the table below.
- 5. Click the **Submit** button; the remote NFS file system is immediately applied, which can be verified by the appearance of the 'NFS mount was successful' message in the Syslog server.
- 6. To save the changes to flash memory, see 'Saving Configuration' on page 470.

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 configuring Web interface tables, see 'Working with Tables' on page 44.
- You can also configure the NFS table using the *ini* file table parameter NFSServers (see 'NFS Parameters' on page 538).



Table 10-15: 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. <ul style="list-style-type: none"> ▪ [2] NFS Version 2 ▪ [3] NFS Version 3 (default)
Authentication Type	Authentication method used for accessing the remote file system. <ul style="list-style-type: none"> ▪ [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. <ul style="list-style-type: none"> ▪ [0] OAM ▪ [1] MEDIA (default) <p>Note: This parameter applies only if VLANs are enabled or if Multiple IPs is configured (see 'Network Configuration' on page 106).</p>

10.9 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.

10.10 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.

10.11 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.

11 Security

This section describes the VoIP security-related configuration.

11.1 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 more 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 556).

➤ To add firewall rules:

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

Figure 11-1: Firewall Settings Page

Edit Rule	Rule Status	Source IP	Source Port	Prefix Length	Local Port Range	Protocol	Use Specific Interface	Interface Name	Packet Size	Byte rate	Burst Bytes	Action Upon Match	Match Count
1	<input checked="" type="radio"/> Not Active	mgmt.customer.com	0	32	0-80	tcp	Enable	Mng	0	0	0	Allow	0
2	<input type="radio"/> Not Active	192.0.0.0	0	9	0-65535	Any	Disable	None	0	40000	50000	ALLOW	0
3	<input type="radio"/> Not Active	10.31.4.0	0	24	4000-9000	Any	Disable	None	0	0	0	BLOCK	0
4	<input type="radio"/> Not Active	10.4.0.0	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 470.
- 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 470.
- **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 470.

Table 11-1: Internal Firewall Parameters

Parameter	Description
Rule Status	Displays (read-only field) whether the rule is active or not. Note: After device reset, all rules are active.
Source IP [AccessList_Source_IP]	Defines the IP address (or DNS name) or a specific host name of the source network (i.e., from where the incoming packet is received).

Parameter	Description
Source Port [AccessList_Source_Port]	<p>Defines the source UDP/TCP ports (on the remote host) from where packets are sent to the device.</p> <p>The valid range is 0 to 65535.</p> <p>Note: When set to 0, this field is ignored and any source port matches the rule.</p>
Prefix Length [AccessList_PrefixLen]	<p>Defines the IP network mask - 32 for a single host or the appropriate value for the source IP addresses.</p> <ul style="list-style-type: none"> ▪ A value of 8 corresponds to IPv4 subnet class A (network mask of 255.0.0.0). ▪ A value of 16 corresponds to IPv4 subnet class B (network mask of 255.255.0.0). ▪ A value of 24 corresponds to IPv4 subnet class C (network mask of 255.255.255.0). <p>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'.</p>
Source Port [AccessList_Source_Port]	<p>Defines the source UDP or TCP ports (on the remote host) from where packets are sent to the device.</p> <p>The valid range is 0 to 65535.</p> <p>Note: When set to 0, this field is ignored and any port matches the rule.</p>
Local Port Range [AccessList_Start_Port] [AccessList_End_Port]	<p>Defines the destination UDP/TCP ports (on this device) to where packets are sent.</p> <p>The valid range is 0 to 65535.</p> <p>Note: When the protocol type isn't TCP or UDP, the entire range must be provided.</p>
Protocol [AccessList_Protocol]	<p>Defines the protocol type (e.g., UDP, TCP, ICMP, ESP or 'Any') or the IANA protocol number in the range of 0 (Any) to 255.</p> <p>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.</p>
Use Specific Interface [AccessList_Use_Specific_Interface]	<p>Determines whether you want to apply the rule to a specific network interface defined in the Multiple Interface table (i.e., packets received from that defined in the Source IP field and received on this network interface):</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Notes:</p> <ul style="list-style-type: none"> ▪ If enabled, then in the 'Interface Name' field (described below), select the interface to which the rule is applied. ▪ If disabled, then the rule applies to all interfaces.
Interface Name [AccessList_Interface_ID]	<p>Defines the network interface to which you want to apply the rule. This is applicable if you enabled the 'Use Specific Interface' field. The list displays interface names as defined in the Multiple Interface table (see 'Configuring IP Interface Settings' on page 102).</p>

Parameter	Description
Packet Size [AccessList_Packet_Size]	Defines the maximum allowed packet size. The valid range is 0 to 65535. Note: When filtering fragmented IP packets, this field relates to the overall (re-assembled) packet size, and not to the size of each fragment.
Byte Rate [AccessList_Byte_Rate]	Defines the expected traffic rate (bytes per second), i.e., the allowed bandwidth for the specified protocol. In addition to this field, the 'Burst Bytes' field provides additional allowance such that momentary bursts of data may utilize more than the defined byte rate, without 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]	Defines the tolerance of traffic rate limit (number of bytes).
Action Upon Match [AccessList_Allow_Type]	Determines the action to be performed upon rule match (i.e., 'Allow' or 'Block').
Match Count [AccessList_MatchCount]	Displays (read-only field) the number of packets accepted and rejected by the specific rule.

11.2 Configuring General Security Settings

The General Security Settings page is used to configure various security features. For a description of the parameters appearing on this page, refer 'Configuration Parameters Reference' on page 529.

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

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

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

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 470.

11.3 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 556).

➤ **To configure IP Security Proposals:**

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

Figure 11-2: 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 470.

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

Table 11-2: IP Security Proposals Table Configuration Parameters

Parameter Name	Description
Encryption Algorithm [IPsecProposalTable_EncryptionAlgorithm]	Determines the encryption (privacy) algorithm. <ul style="list-style-type: none"> ▪ [0] NONE ▪ [1] DES CBC ▪ [2] 3DES CBC ▪ [3] AES (default)
Authentication Algorithm [IPsecProposalTable_AuthenticationAlgorithm]	Determines the message authentication (integrity) algorithm. <ul style="list-style-type: none"> ▪ [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 <i>ini</i> file parameter, X depicts the proposal number (0 to 3). <ul style="list-style-type: none"> ▪ [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 11-3: 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)

11.4 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 556).

➤ **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 11-3: IP Security Associations Table Page

Index	Operational Mode	Remote Endpoint Addr	Authentication Method	Shared Key	Source Port
1	<input type="radio"/> Transport	10.3.2.73	Pre-shared Key	*	0
2	<input type="radio"/> Transport	10.13.4.5	Pre-shared Key	*	0

↓

Destination Port	Protocol	IKE SA Lifetime	IPsec SA Lifetime (Secs)	IPsec SA Lifetime (Kbs)
5070	0	28800	3600	0
0	0	28800	28800	0

↓

Dead Peer Detection Mode	Remote Tunnel Addr	Remote Subnet Addr	Remote Prefix Length	Interface Name
DPD Periodic	0.0.0.0	0.0.0.0	16	None
DPD Disabled	0.0.0.0	0.0.0.0	16	None

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 470.

Table 11-4: IP Security Associations Table Configuration Parameters

Parameter Name	Description
Operational Mode [IPsecSatable_IPsecMode]	Defines the IPSec mode of operation. <ul style="list-style-type: none"> ▪ [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.

Parameter Name	Description
Authentication Method [IPsecSatable_AuthenticationMethod]	<p>Selects the method used for peer authentication during IKE main mode.</p> <ul style="list-style-type: none"> [0] Pre-shared Key (default) [1] RSA Signature = in X.509 certificate <p>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 89.</p>
Shared Key [IPsecSatable_SharedKey]	<p>Defines the pre-shared key (in textual format). Both peers must use the same pre-shared key for the authentication process to succeed.</p> <p>Notes:</p> <ul style="list-style-type: none"> 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 <i>ini</i> 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]	<p>Defines the source port to which this configuration applies. The default value is 0 (i.e., any port).</p>
Destination Port [IPsecSatable_DestPort]	<p>Defines the destination port to which this configuration applies. The default value is 0 (i.e., any port).</p>
Protocol [IPsecSatable_Protocol]	<p>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:</p> <ul style="list-style-type: none"> 0 = Any protocol (default) 17 = UDP 6 = TCP
IKE SA Lifetime [IPsecSatable_Phase1SaLifetimeInSec]	<p>Determines the duration (in seconds) for which the negotiated IKE SA (Main mode) is valid. After this time expires, the SA is re-negotiated.</p> <p>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).</p>
IPsec SA Lifetime (sec) [IPsecSatable_Phase2SaLifetimeInSec]	<p>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).</p> <p>Note: For best performance, a value of 3,600 (i.e., one hour) or more is recommended.</p>

Parameter Name	Description
IPSec SA Lifetime (Kbs) [IPsecSatable_Phase2SaLifetimeKB]	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. <ul style="list-style-type: none"> ▪ [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. <p>Note: For more information on DPD, refer to the <i>Product Reference Manual</i>.</p>
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_RemoteSubnetIP Address]	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 102.

Reader's Notes

12 Media

This section describes the media-related configuration.

12.1 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 529.

➤ **To configure the voice parameters:**

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

Voice Volume (-32 to 31 dB)	<input type="text" value="0"/>
Input Gain (-32 to 31 dB)	<input type="text" value="0"/>
Silence Suppression	<input type="text" value="Disable"/>
DTMF Transport Type	<input type="text" value="RFC2833 Relay DTMF"/>
DTMF Volume (-31 to 0 dB)	<input type="text" value="-11"/>
NTE Max Duration	<input type="text" value="-1"/>
CAS Transport Type	<input type="text" value="CASEventsOnly"/>
DTMF Generation Twist	<input type="text" value="0"/>
Echo Canceller	<input type="text" value="Enable"/>

2. Configure the Voice parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

12.1.1 Voice Gain (Volume) Control

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

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

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

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

Figure 12-1: Voice Volume Parameters in Voice Settings Page

Voice Volume (-32 to 31 dB)	<input type="text" value="0"/>
Input Gain (-32 to 31 dB)	<input type="text" value="0"/>

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

12.1.2 Silence Suppression (Compression)

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

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

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

1. Open the Voice Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Voice Settings**).
2. Set the 'Silence Suppression' (*EnableSilenceCompression*) field to **Enable**.
3. Click **Submit** to apply your changes.

12.1.3 Echo Cancellation

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

In this line echo, echoes are generated when two-wire telephone circuits (carrying both transmitted and received signals on the same wire pair) are converted to a four-wire circuit. Echoes are reflections of the transmitted signal, which result from impedance mismatch in the hybrid (bi-directional 2-wire to 4-wire converting device).

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

The procedure below describes how to configure echo cancellation using the Web interface:

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

4. Open the Voice Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Voice Settings**).
5. Set the 'Echo Canceller' field (*EnableEchoCanceller*) to **Enable**.
6. Open the General Media Settings page (Configuration tab > VoIP menu > Media submenu > General Media Settings).
7. From the 'Max Echo Canceller Length' drop-down list (*MaxEchoCancellerLength*), select the maximum echo path delay (tail length) for the echo canceller.



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

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

12.2 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 144)
- Fax and modem transport modes (see 'Fax/Modem Transport Modes' on page 144)
- V.34 fax support (see 'V.34 Fax Support' on page 149)
- V.152 support (see 'V.152 Support' on page 150)

The fax and modem parameters can be configured in the 'Fax/Modem/CID Settings' page. For a detailed description of the parameters appearing on this page, see 'Configuration Parameters Reference' on page 529.

➤ **To configure the fax and modem parameters:**

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

Figure 12-2: Fax/Modem/CID Settings Page

General Settings	
Fax Transport Mode	RelayEnable
Caller ID Transport Type	Mute
Caller ID Type	Standard Bellcore
V.21 Modem Transport Type	Disable
V.22 Modem Transport Type	Enable Bypass
V.23 Modem Transport Type	Enable Bypass
V.32 Modem Transport Type	Enable Bypass
V.34 Modem Transport Type	Enable Bypass
Fax CNG Mode	Disable
CNG Detector Mode	Disable
Fax Relay Settings	
Fax Relay Redundancy Depth	0
Fax Relay Enhanced Redundancy Depth	4
Fax Relay ECM Enable	Enable
Fax Relay Max Rate (bps)	14400bps
Bypass Settings	
Fax/Modem Bypass Coder Type	G711Alaw_64
Fax/Modem Bypass Packing Factor	1
Fax Bypass Output Gain	0
Modem Bypass Output Gain	0

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.



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 150).

12.2.1 Fax/Modem Operating Modes

The device supports two modes of operation:

- Fax/modem negotiation that is not performed during the establishment of the call.
- Voice-band data (VBD) mode for V.152 implementation (see 'V.152 Support' on page 150): 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`).

12.2.2 Fax/Modem Transport Modes

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

- T.38 fax relay (see 'T.38 Fax Relay Mode' on page 144)
- G.711 Transport: switching to G.711 when fax/modem is detected (see 'G.711 Fax / Modem Transport Mode' on page 145)
- Fax fallback to G.711 if T.38 is not supported (see 'Fax Fallback' on page 146)
- Fax and modem bypass: a proprietary method that uses a high bit rate coder (see 'Fax/Modem Bypass Mode' on page 146)
- NSE Cisco's Pass-through bypass mode for fax and modem (see 'Fax / Modem NSE Mode' on page 147)
- Transparent with events: passing the fax / modem signal in the current voice coder with adaptations (see 'Fax / Modem Transparent with Events Mode' on page 148)
- Transparent: passing the fax / modem signal in the current voice coder (see 'Fax / Modem Transparent Mode' on page 148)
- RFC 2833 ANS Report upon Fax/Modem Detection (see 'RFC 2833 ANS Report upon Fax/Modem Detection' on page 149)

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

12.2.2.1 T.38 Fax Relay Mode

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

T.38 can be configured in the following ways:

- Switching to T.38 mode using SIP Re-INVITE messages (see 'Switching to T.38 Mode using SIP Re-INVITE' on page 145)
- 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 145)

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.

12.2.2.1.1 Switching to T.38 Mode using SIP Re-INVITE

In the Switching to T.38 Mode using SIP Re-INVITE mode, upon detection of a fax signal the terminating device negotiates T.38 capabilities using a Re-INVITE message. If the far-end device doesn't support T.38, the fax fails. In this mode, the 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).

12.2.2.1.2 Automatically Switching to T.38 Mode without SIP Re-INVITE

In the Automatically Switching to T.38 Mode without SIP Re-INVITE mode, when a fax signal is detected, the channel automatically switches from the current voice coder to answer tone mode, and then to T.38-compliant fax relay mode.

To configure automatic T.38 mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 1
- Additional configuration parameters:
 - FaxRelayEnhancedRedundancyDepth
 - FaxRelayRedundancyDepth
 - FaxRelayECMEnable
 - FaxRelayMaxRate

12.2.2.2 G.711 Fax / Modem Transport Mode

In this mode, when the terminating device detects fax or modem signals (CED or AnsAM), it sends a Re-INVITE message to the originating device requesting it to re-open the channel in G.711 VBD with the following adaptations:

- Echo Canceller = off
- Silence Compression = off
- Echo Canceller Non-Linear Processor Mode = off

- Dynamic Jitter Buffer Minimum Delay = 40
- Dynamic Jitter Buffer Optimization Factor = 13

After a few seconds upon detection of fax V.21 preamble or super G3 fax signals, the device sends a second Re-INVITE enabling the echo canceller (the echo canceller is disabled only on modem transmission).

A 'gpmdd' attribute is added to the SDP according to the following format:

- **For G.711A-law:** a=gpmdd:0 vbd=yes;ecan=on (or off, for modems)
- **For G.711 μ -law:** a=gpmdd: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.

12.2.2.3 Fax Fallback

In this mode, when the terminating device detects a fax signal, it sends a Re-INVITE message to the originating device with T.38. If the remote device doesn't support T.38 (replies with SIP response 415 'Media Not Supported'), the device sends a new Re-INVITE with G.711 VBD with the following adaptations:

- Echo Canceller = on
- Silence Compression = off
- Echo Canceller Non-Linear Processor Mode = off
- Dynamic Jitter Buffer Minimum Delay = 40
- Dynamic Jitter Buffer Optimization Factor = 13

When the device initiates a fax session using G.711, a 'gpmdd' attribute is added to the SDP according to the following format:

- **For G.711A-law:** a=gpmdd:0 vbd=yes;ecan=on
- **For G.711 μ -law:** a=gpmdd: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.

12.2.2.4 Fax/Modem Bypass Mode

In this proprietary mode, when fax or modem signals are detected, the channel automatically switches from the current voice coder to a high bit-rate coder (according to the 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

12.2.2.5 Fax / Modem NSE Mode

In this mode, fax and modem signals are transferred using Cisco-compatible Pass-through bypass mode. Upon detection of fax or modem answering tone signal, the terminating device sends three to six special NSE RTP packets (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

12.2.2.6 Fax / Modem Transparent with Events Mode

In this mode, fax and modem signals are transferred using the current voice coder with the following automatic adaptations:

- Echo Canceller = on (or off, for modems)
- Echo Canceller Non-Linear Processor Mode = off
- Jitter buffering optimizations

To configure fax / modem transparent with events mode, perform the following configurations:

- IsFaxUsed = 0
- FaxTransportMode = 3
- V21ModemTransportType = 3
- V22ModemTransportType = 3
- V23ModemTransportType = 3
- V32ModemTransportType = 3
- V34ModemTransportType = 3
- BellModemTransportType = 3

12.2.2.7 Fax / Modem Transparent Mode

In this mode, fax and modem signals are transferred using the current voice coder without notifications to the user and without automatic adaptations. It's possible to use the Profiles mechanism (see 'Coders and Profile Definitions' on page 213) 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 146) or Transparent with Events (see 'Fax / Modem Transparent with Events Mode' on page 148) for modem.

12.2.2.8 RFC 2833 ANS Report upon Fax/Modem Detection

The device (terminator gateway) sends RFC 2833 ANS/ANSam events upon detection of fax and/or modem answer tones (i.e., CED tone). This causes the originator to switch to fax/modem. This parameter is applicable only when the fax or modem transport type is set to bypass, Transparent-with-Events, V.152 VBD, or G.711 transport. When the device is located on the originator side, it ignores these RFC 2833 events

Relevant parameters:

- IsFaxUsed = 0 or 3
- FaxTransportMode = 2
- FaxModemNTEMode = 1
- VxxModemTransportType = 2

12.2.3 V.34 Fax Support

V.34 fax machines can transmit data over IP to the remote side using various methods. The device supports the following modes for transporting V.34 fax data over IP:

- Bypass mechanism for V.34 fax transmission (see 'Bypass Mechanism for V.34 Fax Transmission' on page 149)
- T38 Version 0 relay mode, i.e., fallback to T.38 (see 'Relay Mode for T.30 and V.34 Faxes' on page 150)



Note: The CNG detector is disabled (CNGDetectorMode = 0) in all the subsequent examples.

12.2.3.1 Bypass Mechanism for V.34 Fax Transmission

In this proprietary scenario, the device uses bypass (or NSE) mode to transmit V.34 faxes, enabling the full utilization of its speed.

Configure the following parameters to use bypass mode for both T.30 and V.34 faxes:

- FaxTransportMode = 2 (Bypass)
- V34ModemTransportType = 2 (Modem bypass)
- V32ModemTransportType = 2

- V23ModemTransportType = 2
- V22ModemTransportType = 2

Configure the following parameters to use bypass mode for V.34 faxes and T.38 for T.30 faxes:

- FaxTransportMode = 1 (Relay)
- V34ModemTransportType = 2 (Modem bypass)
- V32ModemTransportType = 2
- V23ModemTransportType = 2
- V22ModemTransportType = 2

12.2.3.2 Relay Mode for T.30 and V.34 Faxes

In this scenario, V.34 fax machines are forced to use their backward compatibility with T.30 faxes and operate in the slower T.30 mode.

Use the following parameters to use T.38 mode for both V.34 and T.30 faxes:

- FaxTransportMode = 1 (Relay)
- V34ModemTransportType = 0 (Transparent)
- V32ModemTransportType = 0
- V23ModemTransportType = 0
- V22ModemTransportType = 0

12.2.4 V.152 Support

The device supports the ITU-T recommendation V.152 (Procedures for Supporting Voice-Band Data over IP Networks). Voice-band data (VBD) is the transport of modem, facsimile, and text telephony signals over a voice channel of a packet network with a codec appropriate for such signals.

For V.152 capability, the device supports T.38 as well as VBD codecs (i.e., G.711 A-law and G.711 μ -law). The selection of capabilities is performed using the coders table (see 'Configuring Coders' on page 213).

When in VBD mode for V.152 implementation, support is negotiated between the device and the remote endpoint at the establishment of the call. During this time, initial exchange of call capabilities is exchanged in the outgoing SDP. These capabilities include whether VBD is supported and associated RTP payload types ('gpmd' SDP attribute), supported codecs, and packetization periods for all codec payload types ('ptime' SDP attribute). After this initial negotiation, no Re-INVITE messages are necessary as both endpoints are synchronized in terms of the other side's capabilities. If negotiation fails (i.e., no match was achieved for any of the transport capabilities), fallback to existing logic occurs (according to the parameter IsFaxUsed).

Below is an example of media descriptions of an SDP indicating support for V.152. In the example, V.152 implementation is supported (using the dynamic payload type 96 and G.711 u-law as the VBD codec) as well as the voice codecs G.711 μ -law and G.729.

```
v=0
o=- 0 0 IN IPV4 <IPAddressA>
s=-
t=0 0
p=+1
c=IN IP4 <IPAddressA
m=audio <udpPort A> RTP/AVP 18 0
a=ptime:10
a=rtpmap:96 PCMU/8000
a=gpmd: 96 vbd=yes
```

Instead of using VBD transport mode, the V.152 implementation can use alternative relay fax transport methods (e.g., fax relay over IP using T.38). The preferred V.152 transport method is indicated by the SDP 'pmft' attribute. Omission of this attribute in the SDP content means that VBD mode is the preferred transport mechanism for voice-band data. To configure T.38 mode, use the CodersGroup parameter.



Note: You can also configure the device to handle G.771 coders received in INVITE SDP offers as VBD coders, using the HandleG711asVBD parameter. For example, if the device is configured with G.729 and G.711 VBD coders and it receives an INVITE with an SDP offer containing G.729 and "regular" G.711 coders, it sends an SDP answer containing G.729 and G.711 VBD coders, allowing subsequent bypass (passthrough) sessions if fax / modem signals are detected during the call.

12.2.5 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.

12.3 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 529.

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

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

▼ General Settings	
Dynamic Jitter Buffer Minimum Delay	<input type="text" value="10"/>
Dynamic Jitter Buffer Optimization Factor	<input type="text" value="10"/>
RTP Redundancy Depth	<input type="text" value="0"/>
Packing Factor	<input type="text" value="1"/>
Basic RTP Packet Interval	<input type="text" value="Default"/> ▼
RFC 2833 TX Payload Type	<input type="text" value="96"/>
RFC 2833 RX Payload Type	<input type="text" value="96"/>
RFC 2198 Payload Type	<input type="text" value="104"/>
Fax Bypass Payload Type	<input type="text" value="102"/>
Enable RFC 3389 CN Payload Type	<input type="text" value="Enable"/> ▼
Comfort Noise Generation Negotiation	<input type="text" value="Enable"/> ▼
Remote RTP Base UDP Port	<input type="text" value="0"/>
⚡ RTP Multiplexing Local UDP Port	<input type="text" value="0"/>
⚡ RTP Multiplexing Remote UDP Port	<input type="text" value="0"/>
⚡ RTP Base UDP Port	<input type="text" value="6000"/>
Analog Signal Transport Type	<input type="text" value="Ignore Analog Signals"/> ▼
▼ RTCP XR Settings	
Burst Threshold	<input type="text" value="-1"/>
Delay Threshold	<input type="text" value="-1"/>
R-Value Delay Threshold	<input type="text" value="-1"/>
⚡ Enable RTCP XR	<input type="text" value="CE_VQMON_DISABLE"/> ▼
Minimum Gap Size	<input type="text" value="16"/>
RTCP XR Report Mode	<input type="text" value="Disable"/> ▼
RTCP XR Packet Interval	<input type="text" value="0"/>
Disable RTCP XR Interval Randomization	<input type="text" value="Disable"/> ▼
RTCP XR Collection Server	<input type="text" value=""/>
RTCP XR Collection Server Transport Type	<input type="text" value="Not Configured"/> ▼

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, refer to 'Saving Configuration' on page 470.

12.3.1 Configuring 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.

The procedure below describes how to configure the jitter buffer using the Web interface.

➤ **To configure jitter buffer using the Web interface:**

1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **RTP/RTCP Settings**).
2. Configure the following parameters:
 - 'Dynamic Jitter Buffer Minimum Delay' (*DJBufMinDelay*) - Defines the minimum delay (in msec) for the Dynamic Jitter Buffer.
 - 'Dynamic Jitter Buffer Optimization Factor' (*DJBufOptFactor*) - Defines the Dynamic Jitter Buffer frame error/delay optimization factor.
3. Click **Submit** to apply your settings.

12.3.2 Comfort Noise Generation

The device can generate artificial background noise ("comfort" noise) in the voice channel during periods of silence (i.e. no party is speaking). This is useful in that it reassures the calling parties that the call is still connected. The device detects silence using its Voice Activity Detection feature. When the CNG is enabled and silence is detected, the device transmits Silence Identifier Descriptors (SIDs) parameters to reproduce the local background noise at the remote (receiving) side.

The Comfort Noise Generation (CNG) support also depends on the silence suppression (SCE) setting for the coder used in the voice channel. For more information, see the description of the CNG-related parameters.

The procedure below describes how to configure CNG using the Web interface.

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

1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **RTP/RTCP Settings**).
2. Set the 'Comfort Noise Generation' (*ComfortNoiseNegotiation*) parameter to **Enable**.
3. Click **Submit** to apply your changes.

12.3.3 Dual-Tone Multi-Frequency Signaling

12.3.3.1 Configuring DTMF Transport Types

The device supports various methods to transport DTMF digits over the IP network to the remote endpoint. These methods and their configuration are described below:

- **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, RFC2833TxPayloadType, and RFC2833RxPayloadType
- MGCPDTMFDetectionPoint, DTMFVolume, DTMFTransportType, DTMFDigitLength, and DTMFInterDigitInterval

12.3.3.2 Configuring RFC 2833 Payload

The procedure below describes how to configure the RFC 2833 payload using the Web interface:

➤ **To configure RFC 2833 payload using the Web interface:**

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

General Settings	
Dynamic Jitter Buffer Minimum Delay	<input type="text" value="10"/>
Dynamic Jitter Buffer Optimization Factor	<input type="text" value="10"/>
RTP Redundancy Depth	<input type="text" value="0"/>
Packing Factor	<input type="text" value="1"/>
Basic RTP Packet Interval	<input type="text" value="Default"/>
RFC 2833 TX Payload Type	<input type="text" value="96"/>
RFC 2833 RX Payload Type	<input type="text" value="96"/>
RFC 2198 Payload Type	<input type="text" value="104"/>
Fax Bypass Payload Type	<input type="text" value="102"/>
Enable RFC 3389 CN Payload Type	<input type="text" value="Enable"/>
Comfort Noise Generation Negotiation	<input type="text" value="Enable"/>
Remote RTP Base UDP Port	<input type="text" value="0"/>
⚡ RTP Multiplexing Local UDP Port	<input type="text" value="0"/>
⚡ RTP Multiplexing Remote UDP Port	<input type="text" value="0"/>
⚡ RTP Base UDP Port	<input type="text" value="6000"/>
Analog Signal Transport Type	<input type="text" value="Ignore Analog Signals"/>
RTCP XR Settings	
Burst Threshold	<input type="text" value="-1"/>
Delay Threshold	<input type="text" value="-1"/>
R-Value Delay Threshold	<input type="text" value="-1"/>
⚡ Enable RTCP XR	<input type="text" value="CE_VQMON_DISABLE"/>
Minimum Gap Size	<input type="text" value="16"/>
RTCP XR Report Mode	<input type="text" value="Disable"/>
RTCP XR Packet Interval	<input type="text" value="0"/>
Disable RTCP XR Interval Randomization	<input type="text" value="Disable"/>
RTCP XR Collection Server	<input type="text" value=""/>
RTCP XR Collection Server Transport Type	<input type="text" value="Not Configured"/>

2. Configure the following parameters:
 - 'RTP Redundancy Depth' (RTPRedundancyDepth) - enables the device to generate RFC 2198 redundant packets.
 - 'Enable RTP Redundancy Negotiation' (EnableRTPRedundancyNegotiation) - enables the device to included the RTP redundancy dynamic payload type in the SDP, according to RFC 2198.
 - 'RFC 2198 Payload Type' (RFC2198PayloadType) - defines the RTP redundancy packet payload type according to RFC 2198.
 - 'RFC 2833 TX Payload Type' (RFC2833TxPayloadType) - defines the Tx RFC 2833 DTMF relay dynamic payload type.
 - 'RFC 2833 RX Payload Type' (RFC2833RxPayloadType) - defines the Rx RFC 2833 DTMF relay dynamic payload type.
3. Click **Submit** to apply your settings.

12.3.4 Configuring 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 152) or to specific IP destinations using the IP Profile feature (see 'Configuring IP Profiles' on page 217).

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.

The procedure below describes how to configure RTP multiplexing using the Web interface.

➤ To configure RTP multiplexing parameters:

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

▼ General Settings	
Dynamic Jitter Buffer Minimum Delay	10
Dynamic Jitter Buffer Optimization Factor	10
RTP Redundancy Depth	0
Packing Factor	1
Basic RTP Packet Interval	Default
RFC 2833 TX Payload Type	96
RFC 2833 RX Payload Type	96
RFC 2198 Payload Type	104
Fax Bypass Payload Type	102
Enable RFC 3389 CN Payload Type	Enable
Comfort Noise Generation Negotiation	Enable
Remote RTP Base UDP Port	0
⚡ RTP Multiplexing Local UDP Port	0
⚡ RTP Multiplexing Remote UDP Port	0
⚡ RTP Base UDP Port	6000
Analog Signal Transport Type	Ignore Analog Signals
▼ RTCP XR Settings	
Burst Threshold	-1
Delay Threshold	-1
R-Value Delay Threshold	-1
⚡ Enable RTCP XR	CE_VQMON_DISABLE
Minimum Gap Size	16
RTCP XR Report Mode	Disable
RTCP XR Packet Interval	0
Disable RTCP XR Interval Randomization	Disable
RTCP XR Collection Server	
RTCP XR Collection Server Transport Type	Not Configured

2. Configure the following parameters:
 - Set the 'RTP Multiplexing Remote UDP Port' (RemoteBaseUDPPort) parameter to a non-zero value.
 - Set the 'RTP Multiplexing Remote UDP Port' (RemoteBaseUDPPort) parameter to the same value set for the 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.
3. Click **Submit**.
4. Reset the device for the settings to take effect.

12.3.5 Configuring RTP Base UDP Port

You can configure the range of UDP ports for RTP, RTCP, and T.38. The UDP port range can be configured using media realms in the Media Realm table, allowing you to assign different port ranges (media realms) to different interfaces. However, if you do not use media realms, you can configure the lower boundary of the UDP port used for RTP, RTCP (RTP port + 1) and T.38 (RTP port + 2), using the 'RTP Base UDP Port' (BaseUDPPort) parameter. For example, if the Base UDP Port is set to 6000, then one channel may use the ports RTP 6000, RTCP 6001, and T.38 6002, while another channel may use RTP 6010, RTCP 6011, and T.38 6012. The range of possible UDP ports is 6,000 to 64,000 (default base UDP port is 6000).

The port range is calculated using the 'RTP Base UDP Port' (BaseUDPPort) parameter as follows: **BaseUDPPort to (BaseUDPPort + <channels -1> * 10)**

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

- BaseUDPPort to (BaseUDPPort + 255*10) - for example, if the BaseUDPPort is set to 6,000, then the UDP port range is 6,000 to 8,550



Notes:

- The device allocates the UDP ports randomly to the channels.
- If you are using Media Realms (see 'Configuring Media Realms' on page 170), the port range configured for the Media Realm must be within this range defined by the BaseUDPPort parameter.

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

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

1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **RTP/RTCP Settings**).
2. Set the 'RTP Base UDP Port' parameter to the required value.
3. Click **Submit**.
4. Reset the device for the settings to take effect.

12.3.6 Configuring RTP Control Protocol Extended Reports (RTCP XR)

RTP Control Protocol Extended Reports (RTCP XR) is a VoIP management control that defines a set of metrics containing information for assessing VoIP call quality and for diagnosing problems. RTCP XR (RFC 3611) extends the RTCP reports defined in RFC 3550 by providing additional VoIP metrics. RTCP XR information publishing is implemented in the device according to <draft-johnston-sipping-rtcp-summary-07>. This draft defines how a SIP User Agent (UA) publishes the detailed information to a defined collector. RTCP XR measures VoIP call quality such as packet loss, delay, signal / noise / echo levels, estimated R-factor, and mean opinion score (MOS). RTCP XR measures these parameters using metrics (refer to the Product Reference Manual).

RTCP XR messages containing key call-quality-related metrics are exchanged periodically (user-defined) between the device and the SIP UA. This allows an analyzer to monitor these metrics midstream, or a device to retrieve them using SNMP. The device can send RTCP XR reports to an Event State Compositor (ESC) server using PUBLISH messages. These reports can be sent at the end of each call (configured using `RTCPXRReportMode`) and according to a user-defined interval (`RTCPInterval` or `DisableRTCPRandomize`) between consecutive reports.

To enable RTCP XR reporting, the `VQMonEnable` ini file parameter must be set to 1. In addition, the device must be installed with the appropriate Software Upgrade Key. For a detailed description of the RTCP XR ini file parameters, refer to the device's User's Manual.

The procedure below describes how to configure RTCP XR using the Web interface.

➤ To configure RTCP XR:

1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **RTP/RTCP Settings**).
2. Configure the following parameters:
 - 'Enable RTCP XR' (`VQMonEnable`) - enables voice quality monitoring and RTCP XR.
 - 'Minimum Gap Size' (`VQMonGMin`) - defines the voice quality monitoring - minimum gap size (number of frames).
 - 'Burst Threshold' (`VQMonBurstTHR`) - defines the voice quality monitoring - excessive burst alert threshold.
 - 'Delay Threshold' (`VQMonDelayTHR`) - defines the voice quality monitoring - excessive delay alert threshold.
 - 'R-Value Delay Threshold' (`VQMonEOCRValTHR`) - defines the voice quality monitoring - end of call low quality alert threshold.
 - 'RTCP XR Packet Interval' (`RTCPInterval`) - defines the time interval between adjacent RTCP reports.
 - 'Disable RTCP XR Interval Randomization' (`DisableRTCPRandomize`) - determines whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter `RTCPInterval`.
 - 'RTCP XR Collection Server Transport Type' (`RTCPXRESCTransportType`) - determines the transport layer for outgoing SIP dialogs initiated by the device to the RTCP-XR Collection Server.
 - 'RTCP XR Collection Server' (`RTCPXREscIP`) - defines the IP address of the Event State Compositor (ESC).
 - 'RTCP XR Report Mode' (`RTCPXRReportMode`) - determines whether RTCP XR reports are sent to the ESC and defines the interval in which they are sent.
3. Click **Submit**.
4. Reset the device for the settings to take effect.

12.4 Configuring IP Media Settings

The IPMedia Settings page allows you to configure the IP media parameters. For a detailed description of the parameters appearing on this page, see 'Configuration Parameters Reference' on page 529.

➤ **To configure the IP media parameters:**

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

IPMedia Settings	
⚡ IPMedia Detectors	Disable
Enable Answer Detector	Disable
Answer Detector Activity Delay	0
Answer Detector Silence Time	10
Answer Detector Redirection	0
Answer Detector Sensitivity	3
Answer Machine Detector Sensitivity Parameter Suit	0
Answer Machine Detector Sensitivity	3
Answer Machine Detector Beep Detection Timeout	200
Answer Machine Detector Beep Detection Sensitivity	0
Enable AGC	Disable
AGC Slope	3
AGC Redirection	0
AGC Target Energy	19
Enable Energy Detector	Disable
Energy Detector Quality Factor	4
Energy Detector Threshold	3
Enable Pattern Detector	Disable
⚡ Active Speakers Min Interval	20
⚡ Number of Media Channels	0
Configure Audio Playback	
Playback Audio Format	PCMA
Configure Audio Recording	
End Of Record Time	60
⚡ Record Audio Format	PCMA

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

12.4.1 Answer Machine Detector (AMD)

The device provides answering machine detection (AMD) capabilities that can detect for example, if a human voice or an answering machine is answering the call. AMD is useful for automatic dialing applications.

The device supports up to four AMD parameter suites, where each parameter suite defines the AMD sensitivity levels of detection. The detection sensitivity levels can range from 0 to 15, depending on parameter suite. The level is selected using the `AMDSensitivityLevel` parameter. The Parameter Suite(s) can be loaded to the device in the Web interface as an auxiliary file (see 'Loading Auxiliary Files' on page 471) or loaded remotely through the ini file (using the `AMDSensitivityFileName` and `AMDSensitivityFileUrl` parameters). In addition,

you can configure AMD per call, based on the called number or Trunk Group. This is achieved by defining the AMD parameters for a specific IP Profile (IPProfile parameter) and then assigning the IP Profile to a Trunk Group in the Inbound IP Routing table (PSTNPrefix parameter).

The device also supports the detection of beeps at the end of an answering machine message. This allows users of third-party, Application servers to leave voice messages after an answering machine plays a “beep” sound.

The device supports two methods for detecting and reporting beeps (configured using the AMDBeepDetectionMode parameter):

- Using the AMD detector. This detector is integrated in the existing AMD feature. The beep detection timeout and beep detection sensitivity are configurable using the AMDBeepDetectionTimeout and AMDBeepDetectionSensitivity parameters respectively.
- Using the Call Progress Tone detector - several beep tones (Tone Type #46) can be configured in the CPT file.

The detection of beeps is done using the X-Detect header extension. The device sends a SIP INFO message containing one of the following field values:

- Type=AMD and SubType=Beep
- Type=CPT and SubType=Beep

Upon every AMD activation, the device can send a SIP INFO message to an Application server notifying it of one of the following:

- Human voice has been detected
- Answering machine has been detected
- Silence (i.e., no voice detected) has been detected

The table below shows the success rates of the AMD feature for correctly detecting live and fax calls:

Table 12-1: Approximate AMD Detection Normal Sensitivity (Based on North American English)

AMD Detection Sensitivity	Performance	
	Success Rate for Live Calls	Success Rate for Answering Machine
0 (Best for Answering Machine)	-	-
1	82.56%	97.10%
2	85.87%	96.43%
3 (Default)	88.57%	94.76%
4	88.94%	94.31%
5	90.42%	91.64%
6	90.66%	91.30%
7 (Best for Live Calls)	94.72%	76.14%

Table 12-2: Approximate AMD Detection High Sensitivity (Based on North American English)

AMD Detection Sensitivity	Performance	
	Success Rate for Live Calls	Success Rate for Answering Machine
0 (Best for Answering Machine)	72%	97%
1	77%	96%
2	79%	95%
3	80%	95%
4	84%	94%
5	86%	93%
6	87%	92%
7	88%	91%
8 (default)	90%	89%
9	90%	88%
10	91%	87%
11	94%	78%
12	94%	73%
13	95%	65%
14	96%	62%
15 (Best for Live Calls)	97%	46%

A pre-requisite for enabling the AMD feature is to set the *ini* file parameter EnableDSPiPMDetectors to 1. In addition, to enable voice detection, required once the AMD detects the answering machine, the *ini* file parameter EnableVoiceDetection must be set to 1.



Note: The device's AMD feature is based on voice detection for North American English. If you want to implement AMD in a different language or region, you must provide AudioCodes with a database of recorded voices in the language on which the device's AMD mechanism can base its voice detector algorithms for detecting these voices. The data needed for an accurate calibration should be recorded under the following guidelines:

- **Statistical accuracy:** The number of recordings should be large (i.e., about 100) and varied. The calls must be made to different people, at different times. The calls must be made in the specific location in which the device's AMD mechanism is to operate.
- **Real-life recording:** The recordings should simulate real-life answering of a person picking up the phone without the caller speaking (until the AMD decision).
- **Normal environment interferences:** The environment should almost simulate real-life scenarios, i.e., not sterile but not too noisy either. Interferences, for example, could include background noises of other people talking, spikes, and car noises.

The SIP call flows below show an example of implementing the device's AMD feature. This scenario example allows a third-party Application server to play a recorded voice message to an answering machine.

1. Upon detection by the device of the answering machine, the device sends a SIP INFO message to the Application server:

```
INFO sip:sipp@172.22.2.9:5060 SIP/2.0
Via: SIP/2.0/UDP 172.22.168.249;branch=z9hG4bKac1566945480
Max-Forwards: 70
From: sut <sip:3000@172.22.168.249:5060>;tag=1c1505895240
To: sipp <sip:sipp@172.22.2.9:5060>;tag=1
Call-ID: 1-29758@172.22.2.9
CSeq: 1 INFO
Contact: <sip:56700@172.22.168.249>
Supported: em,timer,replaces,path,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway/v.6.40A.040.004
Content-Type: application/x-detect
Content-Length: 30
Type= AMD
SubType= AUTOMATA
```

2. The device then detects the start of voice (i.e., the greeting message of the answering machine), and then sends the following to the Application server:

```
INFO sip:sipp@172.22.2.9:5060 SIP/2.0
Via: SIP/2.0/UDP 172.22.168.249;branch=z9hG4bKac482466515
Max-Forwards: 70
From: sut <sip:3000@172.22.168.249:5060>;tag=1c419779142
To: sipp <sip:sipp@172.22.2.9:5060>;tag=1
Call-ID: 1-29753@172.22.2.9
CSeq: 1 INFO
Contact: <sip:56700@172.22.168.249>
Supported: em,timer,replaces,path,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway/v.6.40A.040.004
Content-Type: application/x-detect
Content-Length: 34
Type= PTT
SubType= SPEECH-START
```

3. Upon detection of the end of voice (i.e., end of the greeting message of the answering machine), the device sends the Application server the following:

```

INFO sip:sipp@172.22.2.9:5060 SIP/2.0
Via: SIP/2.0/UDP 172.22.168.249;branch=z9hG4bKac482466515
Max-Forwards: 70
From: sut <sip:3000@172.22.168.249:5060>;tag=1c419779142
To: sipp <sip:sipp@172.22.2.9:5060>;tag=1
Call-ID: 1-29753@172.22.2.9
CSeq: 1 INFO
Contact: <sip:56700@172.22.168.249>
Supported: em,timer,replaces,path,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway/v.6.40A.040.004
Content-Type: application/x-detect
Content-Length: 34
Type= PTT
SubType= SPEECH-END
    
```

4. The Application server now sends its message to the answering message.
If the device detects voice and not an answering machine, the SIP INFO message includes:

```

Type= AMD
SubType= VOICE
    
```

If the device detects silence, the SIP INFO message includes the SubType **SILENT**.

12.4.2 Configuring Automatic Gain Control (AGC)

Automatic Gain Control (AGC) adjusts the energy of the output signal to a required level (volume). This feature compensates for near-far gain differences. AGC estimates the energy of the incoming signal (from the IP or PSTN, determined by the parameter AGCRedirection), calculates the essential gain, and then performs amplification. Feedback ensures that the output signal is not clipped. You can define the required Gain Slope in decibels per second (using the parameter AGCGainSlop) and the required signal energy threshold (using the parameter AGCTargetEnergy).

When the AGC first detects an incoming signal, it begins operating in Fast Mode, which allows the AGC to adapt quickly when a conversation starts. This means that the Gain Slope is 8 dB/sec for the first 1.5 seconds. After this period, the Gain Slope is changed to the user-defined value. You can disable or enable the AGC's Fast Mode feature, using the *ini* file parameter AGCDisableFastAdaptation. After Fast Mode is used, the signal should be off for two minutes in order to have the feature turned on again.



Note: The AGC feature requires that the device be installed with the **IP Media Detectors** Feature Key

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

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

1. Open the IPMedia Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **IPMedia Settings**).
2. Configure the following parameters:
 - 'Enable AGC' (*EnableAGC*) - Enables the AGC mechanism.
 - 'AGC Slope' (*AGCGainSlope*) - Determines the AGC convergence rate.
 - 'AGC Redirection' (*AGCRedirection*) - Determines the AGC direction.
 - 'AGC Target Energy' - Defines the signal energy value (dBm) that the AGC attempts to attain.
3. Click **Submit** to apply your settings.



Note: The following additional parameters can be configured using either the EMS or ini file:

- AGCMinGain - Defines the minimum gain (in dB) by the AGC when activated
- AGCMaxGain - Defines the maximum gain (in dB) by the AGC when activated.
- AGCDisableFastAdaptation - Enables the AGC Fast Adaptation mode

12.5 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 529.

➤ **To configure general media parameters:**

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

Figure 12-3: General Media Settings Page

General Settings	
DSP Version Template Number	0
Max Echo Canceller Length	Default
Enable Continuity Tones	Disable
Nat Traversal	Disable

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

12.6 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 529.

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 12-4: Analog Settings Page

▼ Analog Settings	
⚡ Analog TTX Voltage Level	0.5V
⚡ Analog Metering Type	12 kHz sinusoidal bursts
⚡ Min. Hook-Flash Detection Period [msec]	300
Max. Hook-Flash Detection Period [msec]	700
▼ Coefficients Settings	
⚡ FXS Coefficient Type	USA
⚡ FXO Coefficient Type	USA

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

12.7 Configuring DSP Templates

The DSP Templates page allows you to load up to two DSP templates to the device. In addition, you can define the percentage of DSP resources allocated per DSP template.

➤ **To select DSP templates:**

1. Open the DSP Templates page (**Configuration** tab > **VoIP** menu > **Media** submenu > **DSP Templates**).
2. In the 'Add Index' field, enter the index number to add a new row in the table.
3. In the 'DSP Template Number' field, enter the desired DSP template number.
4. In the 'DSP Resources Percentage' field, enter the desired resource percentage for the specified template.
5. Click **Apply** to save your settings.
6. To save the changes to flash memory, see 'Saving Configuration' on page 470.

**Notes:**

- You must either use the 'DSP Templates page or the DSPVersionTemplateName parameter to select the DSP template, not both. The DSP Templates page must be used only when two concurrent DSP templates are required; the DSPVersionTemplateName parameter must be used only when a single template is used.
- If no entries are defined, the device uses the default DSP template (i.e., Template 0).
- For supported DSP templates, see 'DSP Templates' on page 815.
- For configuring the Web interface's tables, see 'Working with Tables' on page 44.

12.7.1 DSP Channel Resources for SBC/IP-to-IP/IP Media Functionality

The device supports the IP-to-IP call routing application as well as IP media capabilities. The device provides the required DSP resources (channels) for these applications (in addition to the DSP resources needed for the PRI Trunk interfaces). The device provides flexibility in making DSP resources readily available for these applications. This is achieved by employing a method whereby DSP resources are obtained from the interface module itself (i.e., Media Processing Module - MPM), as well as DSP resources "borrowed" from the digital PSTN modules (i.e., TRUNKS module).

**Notes:**

- For the IP-to-IP call routing application, each IP-to-IP call session includes two legs, utilizing two DSP resources.
- In some scenarios, IP-to-IP routing also has the capability of not requiring DSP's.

To enable the IP-to-IP call routing, and/or IP media applications, and to allow optimal management of the required DSP resources, the following needs to be addressed:

- Presence of appropriate Software Upgrade Key
- Suitable hardware configuration
- Correct *ini* file configuration

12.7.1.1 Software Upgrade Keys

Verify (by using the Web interface or downloaded *ini* file) that your device has been supplied with the following Software Upgrade Keys:

- **Number of IPmedia Channels:** this Software Upgrade Key is configured to the maximum number of required DSP resources (e.g., the *ini* file displays "IPMediaDspCh=60").
- **VoicePromptAnnounc(H248.9):** applicable only to IP media capabilities (applicable to all applications).
- **Conf:** applicable only to conferencing IP media capabilities.
- **SBC=<number>:** defines the number of SIP B2BUA sessions (one session for both legs) (Applicable only to the IP-to-IP call routing application.)

12.7.1.2 Hardware Configuration

The device can obtain DSP resources for these applications using one of the following hardware configurations:

- **Media Processing Module (MPM) Modules:** provide DSP resources for IP-to-IP routing, and/or IP media channels for conferencing and IP media functionality. The device can house up to three MPM modules. The DSP resources allocation is as follows:
 - **Without Conferencing:** when the MPM modules are housed in chassis slots 3, 4, and 5, up to 120 DSP resources (without call conferencing) are supported. Each module provides up to 40 DSP resources.
 - **With Conferencing:** when the MPM modules are housed in chassis slots 4, 5, and 6, up to 100 DSP resources are supported with call conferencing (up to 60 conference participants). These channels are allocated as follows:
 - ◆ MPM module in Slot 6 provides 20 channels (and enables conferencing for the device)
 - ◆ MPM modules in slots 4 and 5 each provide 40 channels (i.e., total of 80 channels)



Note: If the device houses all three MPM modules, no other interface module can be housed in the device.

- **PRI Modules:** DSP resources can be obtained from existing TRUNKS modules (i.e., some PSTN interfaces are "disabled").



Note: DSP resources cannot be "borrowed" from PSTN interfaces that use CAS.

- **Combination of MPM and PRI Modules:** DSP resources can be obtained from the MPM and TRUNKS modules (i.e., some PSTN interfaces are "disabled").

For example, to achieve 120 channels (with conferencing), you need to use two MPM modules (inserted in slots 5 and 6) as well as one TRUNKS module providing two PRI spans (in Slot 1).

12.7.1.3 ini File Configuration

The *ini* file must be configured with the following *ini* file parameters:

- **EnableIP2IPApplication:** set to 1 if you want to enable the IP-to-IP call routing application.
- **EnableIPMediaChannels:** set to 1. This (together with the IPMediaDspCh Software Upgrade Key) reduces the number of DSP channels per TRUNKS module. Each DSP typically provides 24 channels for the PRI interface, but this is reduced to 20 channels as described below:
 - TRUNKS module with one Trunk is not affected and still provides 30 channels
 - TRUNKS module with two Trunks is not affected and still provides 60 channels
 - TRUNKS module with four Trunks provides 100 channels (5 DSPs * 20 channels), instead of 120 - cannot be used with MPM modules
- **MediaChannels:** set to the maximum number of required IP media channels (regardless of the module from where the channels are acquired).



Note: Setting the parameter IPmediaChannels to a value that is greater than the available DSP resources from the MPM can result in the "stealing" of DSP resources from the B-channels of the PRI spans.

- **IPmediaChannels:** defines the number of DSP channels that are "borrowed" (used) from each TRUNKS module for IP-to-IP routing, and/or IP media, as shown in the example below:

```
[IPMediaChannels]
FORMAT IPMediaChannels_Index = IPMediaChannels_ModuleID,
IPMediaChannels_DSPChannelsReserved;
IPMediaChannels 1 = 1, 15;
IPMediaChannels 2 = 2, 10;
[ \IPMediaChannels]
```



Notes:

- The value of IPMediaChannels_DSPChannelsReserved must be in multiples of 5.
- By default, the MPM module is set to the maximum number of IP media channels (i.e., no need to define it in the IPmediaChannels table).
- By default, a TRUNKS module is set to 0 (i.e., no IP media channels).

12.8 Configuring Media Realms

The Media Realm Table page allows you to define a pool of up to 64 SIP media interfaces, termed *Media Realms*. Media Realms allow you to divide a Media-type interface (defined in the Multiple Interface table - see 'Configuring IP Interface Settings' on page 102) into several realms, where each realm is specified by a UDP port range. In addition, you can define the maximum number of sessions per Media Realm. Once created, Media Realms can be assigned to IP Groups (in the IP Group table - see 'Configuring IP Groups' on page 193) or SRDs (in the SRD table - see 'Configuring SRD Table' on page 189).

For each Media Realm you can configure Quality of Experience parameters and their thresholds for reporting to the AudioCodes SEM server used for monitoring the quality of calls. For configuring this, see 'Configuring Quality of Experience Parameters per Media Realm' on page 172.



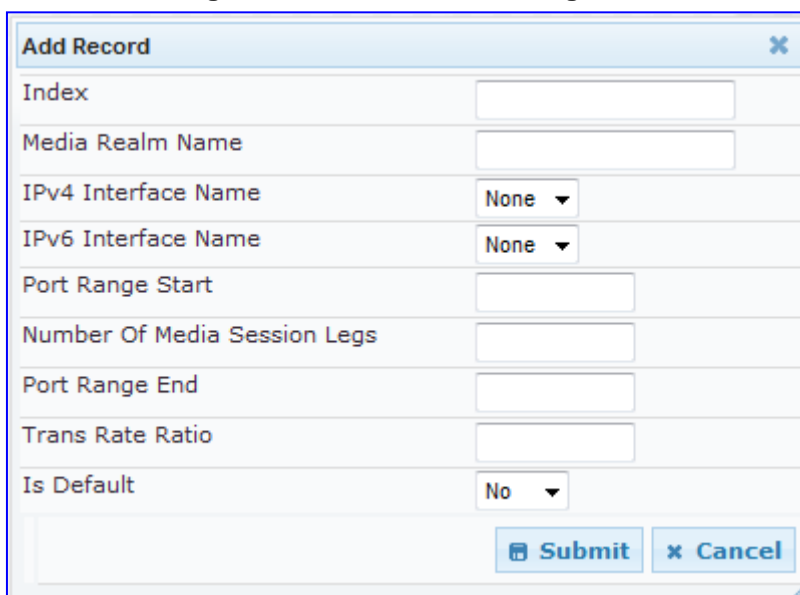
Notes:

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

➤ To define a Media Realm:

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

Figure 12-5: Add Record Dialog Box



Index	<input type="text"/>
Media Realm Name	<input type="text"/>
IPv4 Interface Name	None ▾
IPv6 Interface Name	None ▾
Port Range Start	<input type="text"/>
Number Of Media Session Legs	<input type="text"/>
Port Range End	<input type="text"/>
Trans Rate Ratio	<input type="text"/>
Is Default	No ▾

3. Configure the parameters as required. See the table below for a description of each parameter
4. Click **Submit** to apply your settings.
5. Reset the device to save the changes to flash memory (see 'Saving Configuration' on page 470).

Table 12-3: Media Realm Table Parameter Descriptions

Parameter	Description
Index [CpMediaRealm_Index]	Defines the required table index number.
Media Realm Name [CpMediaRealm_MediaRealmName]	Defines an arbitrary, identifiable name for the Media Realm. The valid value is a string of up to 40 characters. Notes: <ul style="list-style-type: none"> This parameter is mandatory. The name assigned to the Media Realm must be unique. This Media Realm name is used in the SRD and IP Groups table.
IPv4 Interface Name [CpMediaRealm_IPv4IF]	Associates the IPv4 interface with the Media Realm. Note: The name of this interface must be identical (i.e., case-sensitive etc.) as configured in the Multiple Interface table (InterfaceTable parameter).
Port Range Start [CpMediaRealm_PortRangeStart]	Defines the starting port for the range of Media interface UDP ports. Notes: <ul style="list-style-type: none"> You must either configure all media realms with port ranges or without (not some with and some without). The available UDP port range is calculated using the BaseUDPport parameter: <ul style="list-style-type: none"> ✓ BaseUDPport to BaseUDPport + 255*10 Port ranges over 60,000 must not be used. Ranges of Media Realm ports must not overlap.
Number of Media Session Legs [CpMediaRealm_MediaSessionLeg]	Defines the number of media sessions associated with the range of ports. This is the number of media sessions available in the port range. For example, 100 ports correspond to 10 media sessions, since ports are allocated in chunks of 10.
Port Range End [CpMediaRealm_PortRangeEnd]	Read-only field displaying the ending port for the range of Media interface UDP ports. This field is calculated by adding the 'Media Session Leg' field (multiplied by the port chunk size) to the 'Port Range Start' field. A value appears once a row has been successfully added to the table.
Trans Rate Ratio [CpMediaRealm_TransRateRatio]	Note: This field will be supported in the next applicable release.
Is Default [CpMediaRealm_IsDefault]	Defines the Media Realm as the default Media Realm. This default Media Realm is used when no Media Realm is configured for an IP Group or SRD for a specific call. <ul style="list-style-type: none"> [0] No [1] Yes Notes: <ul style="list-style-type: none"> If this parameter is not configured, then the first Media Realm in the table is used as default. If the table is not configured, then the default Media Realm includes all the configured media interfaces.

12.9 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 529.

➤ **To configure media security:**

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

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

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

12.10 Configuring Quality of Experience Parameters per Media Realm

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

For each Media Realm you can specify the call parameters to monitor and configure the upper and lower thresholds, that when exceeded, the device reports the changes in these parameters to the monitoring server. The device can monitor the following parameters:

- Loss
- MOS
- Jitter
- Delay

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

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

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



Notes:

- The QoE feature is available only if the device is installed with the relevant Software Upgrade Key.
- To configure the address of the AudioCodes Session Experience Manager (SEM) server to where the device reports the QoE, see 'Configuring Server for Media Quality of Experience' on page 175.
- You can also use the QOERules *ini* file parameter to configure QoE per Media Realm.

➤ **To configure Quality of Experience per Media Realm:**

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

Figure 12-6: Add Record Dialog Box for QoE

Edit Record	
Index	<input type="text" value="1"/>
Monitored Param	<input type="text" value="Mos"/>
Profile	<input type="text" value="Low Sensitivity"/>
Green Yellow Threshold	<input type="text" value="3.4"/>
Green Yellow Hystersis	<input type="text" value="0.1"/>
Yellow Red Threshold	<input type="text" value="2.7"/>
Yellow Red Hystersis	<input type="text" value="0.1"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

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

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

Table 12-4: Quality of Experience for Media Realm Parameter Descriptions

Parameter	Description
Index [QOERules_RuleIndex]	Defines the table index entry. Up to four entries can be configured per Media Realm.
Monitored Param [QOERules_MonitoredParam]	Defines the parameter to monitor and report. <ul style="list-style-type: none"> ▪ Mos (default) ▪ Delay ▪ PacketLoss ▪ Jitter
Profile [QOERules_Profile]	Defines the pre-configured threshold profile to use. <ul style="list-style-type: none"> ▪ No Profile = No profile is used and you need to define the thresholds in the parameters described below. ▪ Low Sensitivity = Automatically sets the thresholds to low sensitivity values. Therefore, reporting is done only if changes in parameters' values is significant. ▪ Default Sensitivity = Automatically sets the thresholds to a medium sensitivity. ▪ High Sensitivity = Automatically sets the thresholds to high sensitivity values. Therefore, reporting is done for small fluctuations in parameters' values.
Green Yellow Threshold [QOERules_GreenYellowThreshold]	Defines the parameter threshold values between green (good quality) and yellow (medium quality) states.
Green Yellow Hystersis [QOERules_GreenYellowHystersis]	Defines the hysteresis (fluctuation) for the green-yellow threshold. When the threshold is exceeded by this hysteresis value, the device sends a report to the SEM indicating this change.
Yellow Red Threshold [QOERules_YellowRedThreshold]	Defines the parameter threshold values between yellow (medium quality) and red (poor quality). When this threshold is exceeded, the device sends a report to the SEM indicating this change.
Yellow Red Hystersis [QOERules_YellowRedHystersis]	Defines the hysteresis (fluctuation) for the yellow-red threshold. When the threshold is exceeded by this hysteresis value, the device sends a report to the SEM indicating this change.

12.11 Configuring Server for Media Quality of Experience

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

➤ **To configure QoE reporting of media:**

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

Figure 12-7: Media Quality of Experience Page

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

2. Configure the parameters as required
 - 'Server Ip' (QOEServerIP) - defines the IP address of the SEM server
 - 'Port' (QOEPort) - defines the port of the SEM server
 - 'Interface Name' (QOEInterfaceName) - defines the device's IP network interface on which the SEM reports are sent
 - 'Use Mos LQ' (QOEUseMosLQ) - defines the reported MOS type (listening or conversational)
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.



Notes:

- To support this feature, the device must be installed with the relevant Software Upgrade Feature Key.
- To configure the parameters to report and their thresholds per Media Realm, see 'Quality of Experience per Media Realm' on page 172.
- For information on the SEM server, refer to the *EMS User's Manual*.

Reader's Notes

13 Services

This section describes configuration for various supported services.

13.1 Routing Based on LDAP Active Directory Queries

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

The LDAP feature can be configured using the *ini* file, Web interface, SNMP, and CLI (for debugging only).

13.1.1 LDAP Overview

The basic LDAP mechanism is described below:

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

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

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

The address of the LDAP server can be a DNS name (using the `LDAPServerName` parameter) or an IP address (using the `LDAPServerIP` parameter).

- **Search:** To run a search using the LDAP service, the path to the directory's subtree where the search is to be performed must be defined (using the `LDAPSearchDN` parameter). In addition, the search key (known as "filter" in LDAP references), which defines the exact DN to be found and one or more attributes whose values should be returned, must be defined. The device supports up to 20 LDAP search requests.

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

- **CLI:** The LDAP CLI is located in the directory `IPNetworking\OpenLdap`. The following commands can be used:
 - `LdapStatus` - displays connection status
 - `LdapSearch` - searches an LDAP server
 - `LDapOpen` - opens connection to the LDAP server using parameters provided in configuration file
 - `LDapSetDebugmode` - sets the `LdapDebugLevelMode` parameter
 - `LDapGetDebugmode` - gets the `LdapDebugLevelMode` parameter value

Relevant parameters: `LDAPServiceEnable`; `LDAPServerIP`; `LDAPServerDomainName`; `LDAPServerPort`; `LDAPPassword`; `LDAPBindDN`; `LDAPSearchDN`; `LDAPDebugMode`; `LDAPServerMaxRespondTime`.

13.1.2 Configuring LDAP Settings

The LDAP Settings page is used for configuring the Lightweight Directory Access Protocol (LDAP) parameters. For a description of these parameters, see 'Configuration Parameters Reference' on page 529. For an overview of LDAP, see 'Routing Based on LDAP Active Directory Queries' on page 177.

➤ **To configure the LDAP parameters:**

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

Figure 13-1: LDAP Settings Page

LDAP Server Status	Connection Broken
⚡ LDAP Service	Disable <input type="button" value="v"/>
LDAP Server IP	0.0.0.0
LDAP Server Port	389
LDAP Server Max Respond Time	3000
LDAP Server Domain Name	
LDAP Search Dn	
LDAP Password	•••••
LDAP Bind DN	

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

- "Not Applicable"
 - "Connection Broken"
 - "Connecting"
 - "Connected"
2. Configure the parameters as required.
 3. Click **Submit** to apply your changes.
 4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

13.1.3 AD-Based Tel-to-IP Routing in Microsoft OCS 2007 Environment

Typically, enterprises wishing to deploy Microsoft's Office Communication Server 2007 (OCS 2007) are faced with a complex, call routing dial plan when migrating users from their existing PBX/IP-PBX to the OCS 2007 platform. As more and more end-users migrate to the new voice system, dialing plan management and PBX link capacity can be adversely impacted. Moreover, it's easy to perceive that even a temporary failure (or disconnection) of Microsoft's Office Communications Server 2007 Mediation Server (Mediation Server) results in no incoming voice calls from the PBX/IP-PBX/PSTN and therefore, it will be impossible to reach the user on the user's Microsoft Office Communicator (OC) client.

This feature enables the device to make Tel-to-IP call routing decisions based on information stored on Microsoft's Active Directory-based (AD) enterprise directory server. This implements one common, central database to manage and maintain information regarding user's availability, presence, and location.

Based on queries sent to the AD, this feature allows you to route incoming Tel calls to one of the following IP domains:

- PBX/IP-PBX (for users yet to migrate to the OCS 2007 platform)
- OCS clients (clients connected to the OCS 2007 platform)
- Mobile

The device queries the AD using the destination number. The device's AD queries return up to three user phone number IP destinations, each pertaining to one of the IP domains listed above. The device routes the call according to the following priority:

1. **OCS SIP address:** The call is routed to Mediation Server (which then routes the call to the OCS client).
2. **Mobile number:** If the Mediation Server or OCS client is unavailable (e.g., SIP response 404 "Not Found" upon INVITE sent to OCS client), the device routes the call to the user's mobile number (if exists in the AD).
3. **PBX/IP-PBX number:** If no OCS client exists in the AD, then the device routes the call to the PBX/IP-PBX (if this fails, the call is routed to the mobile number, if exists).

For enterprises implementing a PBX/IP-PBX system but yet to migrate to the OCS 2007 platform, if the PBX/IP-PBX system is unavailable, the device queries the AD for the users mobile phone number and then routes the call, through the PSTN to the mobile destination.

This feature is configured in the Outbound IP Routing table, where the "LDAP" keywords are entered for the destination phone prefixes. For each IP domain (listed above), the destination numbers are prefixed (case-sensitive) as follows:

- **OCS client number:** "OCS:"
- **PBX number:** "PBX:"
- **Mobile number:** "MOBILE:"
- **LDAP failure:** "LDAP_ERR:"

Note that these prefixes are only involved in the routing and manipulation stages; they are not used as the final destination number.

In addition, once you have configured the LDAP parameters (see 'LDAP Overview' on page 177), you need to enter the "LDAP" value for the destination IP address of the LDAP server in the Outbound IP Routing table.

For enabling alternative routing, you need to enable the alternative routing mechanism and configure corresponding SIP reasons for alternative routing. For this feature, alternative routing always starts again from the top of the table (first routing rule entry) and not from the next row.

This feature uses the following parameters to configure the attribute names in the AD used in the LDAP query:

- AD attribute for Mediation Server: MSLDAPOCSNumAttributeName (the default is "msRTCSIPPrimaryUserAddress")
- AD attribute for PBX/IP-PBX: MSLDAPPBXNumAttributeName (the default is "telephoneNumber")
- AD attribute for mobile number: MSLDAPMobileNumAttributeName (the default is "mobile")

Below is an example for configuring AD-based routing rules in the Outbound IP Routing Table (see 'Configuring Outbound IP Routing Table' on page 269):

Figure 13-2: Active Directory-based Routing Rules in Outbound IP Routing Table

Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	- >	Dest. IP Address	Port
*	PBX:	*		10.33.45.65	
*	OCS:	*		10.33.45.68	
*	MOBILE:	*		10.33.45.100	
*	LDAP_ERR	*		10.33.45.80	
*	*	*		LDAP	
*	*	*		10.33.45.72	

- **First rule:** sends call to IP-PBX (10.33.45.65) if AD query replies with prefix "PBX:"
- **Second rule:** sends call to OCS client (i.e., Mediation Server at 10.33.45.68) if AD query replies with prefix "OCS:"
- **Third rule:** sends call to users mobile phone number (to PSTN through the device's IP address, 10.33.45.100) if AD query replies with prefix "MOBILE:"
- **Fourth rule:** sends call to IP address of device, for example (10.33.45.80) if no response from LDAP server
- **Fifth rule:** sends query of received Tel destination number to LDAP server, and then routes the call according to query reply and routing rules at top of table.
- **Sixth rule:** if LDAP functionality is not enabled, routes calls to IP address 10.33.45.72

Therefore, once the device receives the incoming Tel call, the first rule that it uses is the fifth rule, which queries the AD server. When the AD replies, the device searches the table from the first rule down for the matching destination phone prefix (i.e., "PBX:", "OCS:", "MOBILE:", and "LDAP_ERR:"), and then sends the call to the appropriate destination.

13.2 Least Cost Routing

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

13.2.1 Overview

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

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

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

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

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

Table 13-1: Call Cost Comparison between Cost Groups for different Call Durations

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

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

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

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

Two Cost Groups are configured as shown below:

Table 13-2: Configured Cost Groups for Local and International Calls

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

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

Table 13-3: Cost Groups Assigned to Outbound IP Routing Rules for Local and International Calls

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

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

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

- The following Cost Groups are configured:

Table 13-4: Configured Cost Groups

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

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

Table 13-5: Cost Groups Assigned to Outbound IP Routing Rules

Routing Index	Dest Phone Prefix	Destination IP	Cost Group ID
1	201	x.x.x.x	"A"
2	201	x.x.x.x	"B"
3	201	x.x.x.x	0
4	201	x.x.x.x	"B"

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

- Index 1 - Cost Group "A" has the lowest connection cost and minute cost
- Index 2 - Cost Group "B" takes precedence over Index 4 entry based on the first-matched method rule

- Index 3 - no Cost Group is assigned, but as the Default Cost parameter is set to **Min**, it is selected as the cheapest route
 - Index 4 - Cost Group "B" is only second-matched rule (Index 1 is the first)
- **Example 3:** This example shows how the cost of a call is calculated if the call spans over multiple time bands:

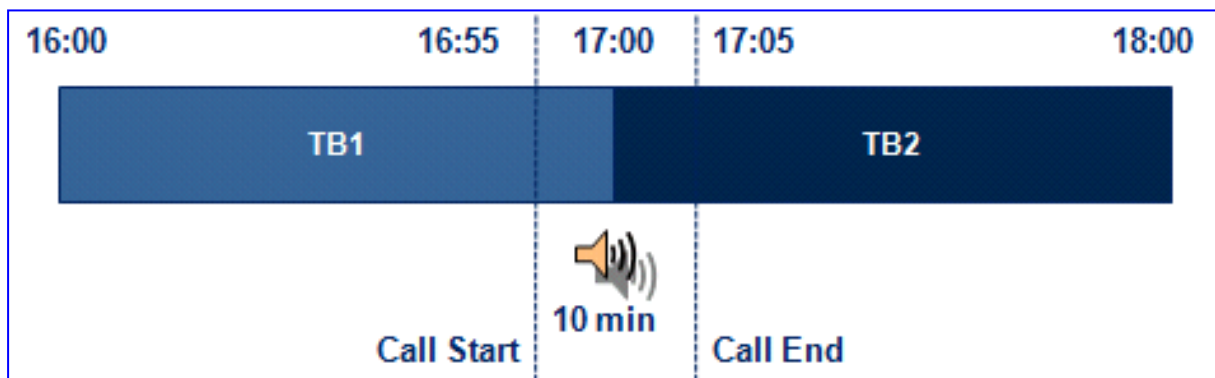
Assume a Cost Group, "CG Local" is configured with two time bands, as shown below:

Table 13-6: Cost Group with Multiple Time Bands

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

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

Figure 13-3: LCR using Multiple Time Bands (Example)



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

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

13.2.2 Configuring LCR

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

1. Enable the LCR feature and configure the average call duration and default call connection cost - see 'Enabling the LCR Feature' on page 184.
2. Configure Cost Groups - see 'Configuring Cost Groups' on page 186.
3. Configure Time Bands for a Cost Group - see 'Configuring Time Bands for Cost Groups' on page 187.
4. Assign Cost Groups to outbound IP routing rules - see 'Assigning Cost Groups to Routing Rules' on page 188.

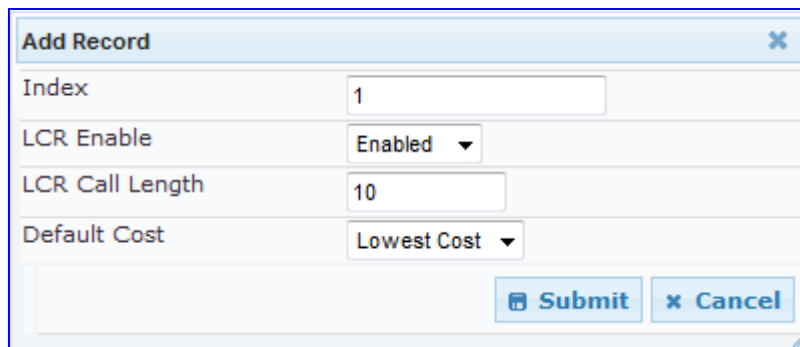
13.2.2.1 Enabling the LCR Feature

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

➤ **To enable LCR:**

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

Figure 13-4: Routing Rule Groups Table - Add Record



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

Table 13-7: Routing Rule Groups Table Description

Parameter	Description
Index [RoutingRuleGroups_Index]	Defines the table index entry. Note: Only one index entry can be configured.
LCR Enable [RoutingRuleGroups_LCR Enable]	Enables the LCR feature: <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable

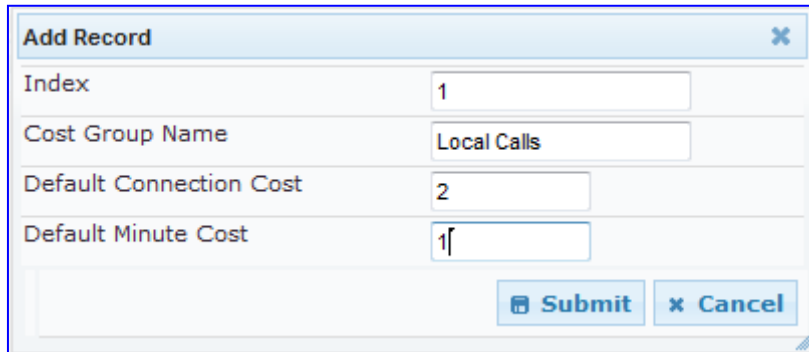
Parameter	Description
LCR Call Length [RoutingRuleGroups_LCR AverageCallLength]	<p>Defines the average call duration (in minutes) and is used to calculate the variable portion of the call cost. This is useful, for example, when the average call duration spans over multiple time bands. The LCR is calculated as follows: $\text{cost} = \text{call connect cost} + (\text{minute cost} * \text{average call duration})$</p> <p>The valid value range is 0-65533. the default is 1.</p> <p>For example, assume the following Cost Groups:</p> <ul style="list-style-type: none"> ▪ "Weekend A": call connection cost is 1 and charge per minute is 6. Therefore, a call of 1 minute cost 7 units. ▪ "Weekend_B": call connection cost is 6 and charge per minute is 1. Therefore, a call of 1 minute cost 7 units. <p>Therefore, for calls under one minute, "Weekend A" carries the lower cost. However, if the average call duration is more than one minute, then "Weekend B" carries the lower cost.</p>
Default Cost [RoutingRuleGroups_LCR DefaultCost]	<p>Determines whether routing rules in the Outbound IP Routing table without an assigned Cost Group are considered a higher cost or lower cost route compared to other matched routing rules that are assigned Cost Groups.</p> <ul style="list-style-type: none"> ▪ [0] Min = If the device locates other matching LCR routing rules, this routing rule is considered the lowest cost route and therefore, it is selected as the route to use (default.) ▪ [1] Max = If the device locates other matching LCR routing rules, this routing rule is considered as the highest cost route and therefore, is not used or used only if the other cheaper routes are unavailable. <p>Note: If more than one valid routing rule without a defined Cost Group exists, the device selects the first-matched rule.</p>

13.2.2.2 Configuring Cost Groups

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

➤ **To configure Cost Groups:**

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



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

Table 13-8: Cost Group Table Description

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

13.2.2.3 Configuring Time Bands for Cost Groups

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



Note: You cannot define overlapping time bands.

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

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

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

Table 13-9: Time Band Table Description

Parameter	Description
Index [CostGroupTimebands_TimebandIndex]	Defines the table index entry.
Start Time [CostGroupTimebands_StartTime]	<p>Defines the day and time of day from when this time band is applicable. The format is ddd:hh:mm (e.g., sun:06:00), where:</p> <ul style="list-style-type: none"> ▪ <i>ddd</i> is the day (i.e., sun, mon, tue, wed, thu, fri, or sat) ▪ <i>hh</i> and <i>mm</i> denote the time of day, where <i>hh</i> is the hour (00-23) and <i>mm</i> the minutes (00-59)

Parameter	Description
End Time [CostGroupTimebands_EndTime]	Defines the day and time of day until when this time band is applicable. For a description of the valid values, see the parameter above.
Connection Cost [CostGroupTimebands_ConnectionCost]	Defines the call connection cost during this time band. This is added as a fixed charge to the call. The valid value range is 0-65533. The default is 0. Note: The entered value must be a whole number (i.e., not a decimal).
Minute Cost [CostGroupTimebands_MinuteCost]	Defines the call cost per minute charge during this timeband. The valid value range is 0-65533. The default is 0. Note: The entered value must be a whole number (i.e., not a decimal).

13.2.2.4 Assigning Cost Groups to Routing Rules

Once you have configured your Cost Groups, you need to assign them to routing rules in the Outbound IP Routing table. For more information, see 'Configuring Outbound IP Routing Table' on page [269](#).

14 Control Network

This section describes configuration of the network at the SIP control level.

14.1 Configuring SRD Table

The SRD Settings page allows you to configure up to 32 signaling routing domains (SRD). An SRD is configured with a unique name and assigned a Media Realm (defined in the Media Realm table - see 'Configuring Media Realms' on page 170). Once configured, you can use the SRDs as follows:

- Associate it with a SIP Interface (see 'Configuring SIP Interface Table' on page 191)
- Associate it with an IP Group (see Configuring IP Groups on page 193)
- Associate it with a Proxy Set (see Configuring Proxy Sets Table on page 198)
- Use it as a destination IP-to-IP routing rule (see Configuring IP-to-IP Routing Table)

Therefore, an SRD is a set of definitions together creating multiple, virtual multi-service IP gateways:

- Multiple and different SIP signaling interfaces (SRD associated with a SIP Interface) and RTP media (associated with a Media Realm) for multiple Layer-3 networks.
- Can operate with multiple gateway customers that may reside either in the same or in different Layer-3 networks as the device. This allows separation of signaling traffic between different customers. In such a scenario, the device is configured with multiple SRD's.

Typically, one SRD is defined for each group of SIP UAs (e.g. proxies, IP phones, application servers, gateways, and softswitches) that communicate with each other. This provides these entities with VoIP services that reside on the same Layer-3 network (must be able to communicate without traversing NAT devices and must not have overlapping IP addresses). Routing from one SRD to another is possible, whereby each routing destination (IP Group or destination address) indicates the SRD to which it belongs.

The SRD Settings page also displays the IP Groups, Proxy Sets, and SIP Interfaces associated with a selected SRD index.

**Notes:**

- For a detailed description of SRD's, see 'Multiple SIP Signaling/Media Interfaces Environment' on page 204.
- The SRD table can also be configured using the *ini* file table parameter SRD.

➤ To configure SRDs:

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

SRD Settings

SRD Index 0 - LAN_srd

Common Parameters

SRD Name LAN_srd

Media Realm LAN_media_realm

IP Group Status Table

Index	Type	Description	Proxy set ID	SIP group name	IP profile ID
1	USER	LAN_users	-1		0

Proxy Sets Status Table

Index	Enable Proxy Keep Alive
0	Disable

X Remove
 ✓ Submit

SIP Interface Table

Add

Note: Select row button to modify the relevant row.

	Network Interface	Application Type	UDP Port	TCP Port	TLS Port
<input type="radio"/>	Voice	GW/VP2IP	5080	5080	5081

2. From the 'SRD Index' drop-down list, select an index for the SRD, and then configure it according to the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.



Note: The SRD Settings page also allows you to define a SIP Interface in the SIP Interface table, instead of navigating to the SIP Interface Table page as described in 'Configuring SIP Interface Table' on page 191.

Table 14-1: SRD Table Parameters

Parameter	Description
SRD Name [SRD_Name]	Mandatory descriptive name of the SRD. The valid value can be a string of up to 21 characters.
Media Realm [SRD_MediaRealm]	Defines the Media Realm associated with the SRD. The entered string value must be identical (including case-sensitive) to the Media Realm name as defined in the Media Realm table. The valid value is a string of up to 40 characters. Notes: <ul style="list-style-type: none"> ▪ If the Media Realm is later deleted from the Media Realm table, then

Parameter	Description
	<p>this value becomes invalid in the SRD table.</p> <ul style="list-style-type: none"> For configuring Media Realms, see 'Configuring Media Realms' on page 170.

14.2 Configuring SIP Interface Table

The SIP Interface Table page allows you to configure up to 32 SIP signaling interfaces, referred to as *SIP Interfaces*. A SIP Interface consists of a combination of ports (UDP, TCP, and TLS), associated with a specific IP address (IPv4), and for a specific application (i.e., SAS, Gateway\IP2IP). Once defined, the SIP Interface can then be associated with an SRD (in the SRD Settings page - see 'Configuring SRD Table' on page 189).

SIP Interfaces can be used for the following:

- Implementing SIP signaling interfaces for each call leg (i.e., each SIP UA communicates with a specific SRD).
- Implementing different SIP signaling ports (listening UDP, TCP, and TLS, and the UDP source ports) for a single interface or for multiple interfaces.
- Differentiating between applications (i.e., SAS, Gateway\IP2IP) by creating SIP Interfaces per application.
- Separating signaling traffic between networks (e.g., different customers) to use different routing tables, manipulations, SIP definitions, and so on.



Notes:

- The SIP Interface table also appears in the SRD Settings page, allowing you to add SIP Interfaces there as well.
- For more information on SIP interfaces, see 'Multiple SIP Signaling/Media Interfaces Environment' on page 204.
- The SIP Interface table can also be configured using the *ini* file table parameter SIPInterface.

➤ To configure the SIP Interface table:

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SIP Interface Table**).

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	<input type="radio"/> SIP1	GW\IP2IP	<input type="text" value="5060"/>	<input type="text" value="5060"/>	<input type="text" value="5061"/>	<input type="text" value="0"/>
2	<input type="radio"/> SIP2	SAS	<input type="text" value="5080"/>	<input type="text" value="5080"/>	<input type="text" value="5081"/>	<input type="text" value="1"/>

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 470.

Table 14-2: SIP Interface Table Parameters

Parameter	Description
Network Interface [SIPInterface_NetworkInterface]	Defines the Control-type IP network interface that you want to associate with the SIP Interface. This value string must be identical (including case-sensitive) to that configured in the 'Interface Name' in the Multiple Interface table (see 'Configuring IP Interface Settings' on page 102). The default is "Not Configured". Note: SIP Interfaces that are assigned to a specific SRD must be defined with the same network interface. For example, if you define three SIP Interfaces for SRD ID #8, all these SIP Interfaces must be defined with the same network interface (e.g., "SIP1").
Application Type [SIPInterface_ApplicationType]	Defines the application type associated with the SIP Interface. <ul style="list-style-type: none"> ▪ [0] GW/IP2IP (default) = IP-to-IP routing application and regular gateway functionality ▪ [1] SAS = Stand-Alone Survivability (SAS) application
UDP Port [SIPInterface_UDPPort]	Defines the listening and source UDP port. The valid range is 1 to 65534. The default is 5060. Notes: <ul style="list-style-type: none"> ▪ This port must be outside of the RTP port range. ▪ Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).
TCP Port [SIPInterface_TCPPort]	Defines the listening TCP port. The valid range is 1 to 65534. The default is 5060. Notes: <ul style="list-style-type: none"> ▪ This port must be outside of the RTP port range. ▪ Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).
TLS Port [SIPInterface_TLSPort]	Defines the listening TLS port. The valid range is 1 to 65534. The default is 5061. Notes: <ul style="list-style-type: none"> ▪ This port must be outside of the RTP port range. ▪ Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).
SRD [SIPInterface_SRD]	Defines the SRD ID associated with the SIP Interface. The default SRD is 0. Notes: <ul style="list-style-type: none"> ▪ Each SRD can be associated with up to two SIP Interfaces, where each SIP Interface pertains to a different Application Type (GW/IP2IP, SAS,). ▪ SIP Interfaces that are assigned to a specific SRD must be defined with the same network interface. For example, if you define three SIP Interfaces for SRD ID #8, all these SIP Interfaces must be defined with the same network interface (e.g., "SIP1"). ▪ To configure SRDs, see 'Configuring SRD Table' on page 189.

14.3 Configuring IP Groups

The IP Group Table page allows you to create up to 32 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 198), 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 table (see 'Configuring Account Table' on page 223).
- 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 Outbound IP Routing Table). For Tel-to-IP calls, the IP Group (*Serving IP Group*) can be used as the IP destination to where all SIP dialogs that are initiated from a Trunk Group are sent (defined in 'Configuring Trunk Group Settings' on page 251).
 - 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).
- If different SRDs are configured in the IP Group and Proxy Set tables, the SRD defined for the Proxy Set takes precedence.
- 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 'Configuration Parameters Reference' on page 529).

➤ **To configure IP Groups:**

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

Index	0
Common Parameters	
Type	SERVER
Description	
Proxy Set ID	
SIP Group Name	
Contact User	
SRD	0
Media Realm	
IP Profile ID	0
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	

2. Configure the IP group parameters according to the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

Table 14-3: IP Group Parameters

Parameter	Description
Common Parameters	
Type [IPGroup_Type]	<p>The IP Group can be defined as one of the following types:</p> <ul style="list-style-type: none"> ▪ [0] SERVER = used when the destination address (configured by the Proxy Set) of the IP Group (e.g., ITSP, Proxy, IP-PBX, or Application server) is known. ▪ [1] USER = represents a group of users (such as IP phones and softphones) where their location is dynamically obtained by the device when REGISTER requests and responses traverse (or are terminated) by the device. These users are considered remote (far-end) users. <p>Typically, this IP Group is configured with a Serving IP Group that represents an IP-PBX, Application or Proxy server that serves this USER-type IP Group. Each SIP request sent by a user of this IP Group is proxied to the Serving IP Group. For registrations, the device updates its internal database with the AOR and contacts of the users.</p> <p>Digest authentication using SIP 401/407 responses (if needed) is performed by the Serving IP Group. The device forwards these responses directly to the SIP users.</p>

Parameter	Description
	<p>To route a call to a registered user, a rule must be configured in the Outbound IP Routing Table table (see Configuring Outbound IP Routing Table on page 269). The device searches the dynamic database (by using the request URI) for an entry that matches a registered AOR or Contact. Once an entry is found, the IP destination is obtained from this entry, and a SIP request is sent to the destination. The device supports up to 600 registered users. The device also supports NAT traversal for the SIP clients that are behind NAT. In this case, the device must be defined with a global IP address.</p> <p>Note: This field is available only if the IP-to-IP application is enabled.</p>
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 198) associated with the IP Group. All INVITE messages destined to this IP Group are sent to the IP address associated with the Proxy Set. <p>Notes:</p> <ul style="list-style-type: none"> ▪ Proxy Set ID 0 must not be selected; this is the device's default Proxy. ▪ The Proxy Set is applicable only to SERVER-type IP Groups.
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 226) is used instead. The value range is a string of up to 100 characters. The default is an empty field. <p>Note: If the IP Group is of type USER, this parameter is used internally as a host name in the Request-URI for Tel-to-IP initiated calls. For example, if an incoming call from the device's T1 trunk is routed to a USER-type IP Group, the device first creates the Request-URI (<destination_number>@<SIP Group Name>), and then it searches the user's internal database for a match.</p>
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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only to SERVER-type IP Groups. ▪ This parameter is overridden by the 'Contact User' parameter in the 'Account' table (see 'Configuring Account Table' on page 223).
SRD [IPGroup_SRD]	The SRD (defined in Configuring SRD Table on page 189) associated with the IP Group. The default is 0. <p>Note: For this parameter to take effect, a device reset is required.</p>

Parameter	Description
Media Realm [IPGroup_MediaRealm]	Associates a Media Realm with the IP Group. The entered string value must be identical (including case-sensitive) to the Media Realm name as defined in the Media Realm table. Notes: <ul style="list-style-type: none"> For this parameter to take effect, a device reset is required. If the Media Realm is later deleted from the Media Realm table, then this value becomes invalid. For configuring Media Realms, see Configuring Media Realms on page 170.
IP Profile ID [IPGroup_ProfileId]	The IP Profile (defined in to 'Configuring IP Profile Settings' on page 217) 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. <ul style="list-style-type: none"> [0] No (default). [1] Yes = The device uses the IP address (or domain name) defined in the Outbound IP Routing Table' (see 'Configuring the Outbound IP Routing Table' on page 269) as the Request-URI host name in outgoing INVITE messages instead of the value entered in the 'SIP Group Name' field. Note: This parameter is applicable only to SERVER-type IP Groups.
Routing Mode [IPGroup_RoutingMode]	Defines the routing mode for outgoing SIP INVITE messages. <ul style="list-style-type: none"> [-1] Not Configured = The routing is according to the selected Serving IP Group. If no Serving IP Group is selected, the device routes the call according to the Outbound IP Routing Table' (see Configuring Outbound IP Routing Table on page 269). (Default) [0] Routing Table = The device routes the call according to the Outbound IP Routing Table'. [1] Serving IP Group = The device sends the SIP INVITE to the selected Serving IP Group. If no Serving IP Group is selected, the default IP Group is used. If the Proxy server(s) associated with the destination IP Group is not alive, the device uses the Outbound IP Routing Table' (if the parameter IsFallbackUsed is set 1, i.e., fallback enabled - see Configuring Proxy and Registration Parameters on page 226). [2] Request-URI = The device sends the SIP INVITE to the IP address according to the received SIP Request-URI host name. Notes: <ul style="list-style-type: none"> This parameter is applicable only if the IP-to-IP application is enabled. This parameter is applicable only to SERVER-type IP Groups.
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). <ul style="list-style-type: none"> [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

Parameter	Description
	<p>AlwaysSendtoProxy is set to 0.</p> <ul style="list-style-type: none"> ▪ [2] Routing Table = Uses the Routing table to locate the destination and then sends a new INVITE to this destination. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.
<p>Enable Survivability [IPGroup_EnableSurvivability]</p>	<p>Determines whether Survivability mode is enabled for USER-type IP Groups.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable if Necessary = Survivability mode is enabled. The device records in its database the registration messages sent by the clients belonging to the USER-type IP Group. If communication with the Serving IP Group (e.g., IP-PBX) fails, the USER-type IP Group enters into Survivability mode in which the device uses its database for routing calls between the clients (e.g., IP phones) of the USER-type IP Group. The RTP packets between the IP phones in Survivability mode always traverse through the device. In Survivability mode, the device is capable of receiving new registrations. When the Serving IP Group is available again, the device returns to normal mode, sending INVITE and REGISTER messages to the Serving IP Group. ▪ [2] Always Enable = Survivability mode is always enabled. The communication with the Serving IP Group (e.g., IP-PBX) is always considered as failed. The device uses its database for routing calls between the clients (e.g., IP phones) of the USER-type IP Group. <p>Notes:</p> <ul style="list-style-type: none"> ▪ This field is available only if the IP-to-IP application is enabled. ▪ This parameter is applicable only to USER-type IP Groups.
<p>Serving IP Group ID [IPGroup_ServingIPGroup]</p>	<p>If configured, INVITE messages initiated from the IP Group are sent to this Serving IP Group (range 1 to 9). In other words, the INVITEs are sent to the address defined for the Proxy Set associated with this Serving IP Group. The Request-URI host name in the INVITE messages are set to the value of the 'SIP Group Name' parameter defined for the Serving IP Group.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This field is available only if the IP-to-IP application is enabled. ▪ If the parameter PreferRouteTable is set to 1, the routing rules in the 'Outbound IP Routing Table' takes precedence over this 'Serving IP Group ID' parameter. ▪ If this parameter is not configured, the INVITE messages are sent to the default Proxy or according to the 'Outbound IP Routing Table'.

14.4 Configuring Proxy Sets Table

The Proxy Sets Table page allows you to define *Proxy Sets*. A Proxy Set is a group of Proxy servers defined by IP address or fully qualified domain name (FQDN). You can define up to 32 Proxy Sets, each with 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 193). When the device sends an INVITE message to an IP Group, it is sent to the IP address or domain name defined for the Proxy Set that is associated with the IP Group. In other words, the Proxy Set represents the **destination** of the call. Typically, for IP-to-IP call routing, at least two Proxy Sets are defined for call destination – one for each leg (IP Group) of the call (i.e., both directions). For example, one Proxy Set for the Internet Telephony Service provider (ITSP) interfacing with one 'leg' of the device and another Proxy Set for the second SIP entity (e.g., ITSP) interfacing with the other 'leg' of the device.



Notes:

- You can also configure the Proxy Sets table using two complementary *ini* file table parameters (see 'Configuration Parameters Reference' on page 529):
 - 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 14-1: Proxy Sets Table Page

Proxy Set ID: 1

	Proxy Address	Transport Type
1	100.33.2.26	UDP
2		
3		
4		
5		

Enable Proxy Keep Alive: Disable
 Proxy Keep Alive Time: 10
 Proxy Load Balancing Method: Round Robin
 Is Proxy Hot Swap: No
 Proxy Redundancy Mode: Not Configured
 SRD Index: 1
 Classification Input: IP only

2. From the 'Proxy Set ID' drop-down list, select an ID for the desired group.
3. Configure the Proxy parameters according to the following table.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 470.

Table 14-4: Proxy Sets Table Parameters

Parameter	Description
Web: Proxy Set ID EMS: Index [ProxySet_Index]	<p>The Proxy Set identification number. The valid range is 0 to 31. The Proxy Set ID 0 is used as the default Proxy Set.</p> <p>Note: Although not recommended, you can use both default Proxy Set (ID 0) and IP Groups for call routing. For example, in the Trunk Group Settings page (see 'Configuring Trunk Group Settings' on page 251) you can configure a Serving IP Group to where you want to route specific Trunk Group channels, and all other device channels then use the default Proxy Set. You can also use IP Groups in the Outbound IP Routing Table (see 'Configuring the Outbound IP Routing Table' on page 269) to configure the default Proxy Set if the parameter PreferRouteTable is set to 1.</p> <p>To summarize, if the default Proxy Set is used, the INVITE message is sent according to the following preferences:</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ To the Trunk Group's Serving IP Group ID, as defined in the Trunk Group Settings table. ▪ According to the Outbound IP Routing Table if the parameter PreferRouteTable is set to 1. ▪ To the default Proxy. <p>Typically, when IP Groups are used, there is no need to use the default Proxy, and all routing and registration rules can be configured using IP Groups and the Account tables (see 'Configuring Account Table' on page 223).</p>
Proxy Address [ProxyIp_IpAddress]	<p>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>.</p> <p>If you enable Proxy Redundancy (by setting the parameter EnableProxyKeepAlive to 1 or 2), the device can operate with multiple Proxy servers. If there is no response from the first (<i>primary</i>) Proxy defined in the list, the device attempts to communicate with the other (<i>redundant</i>) Proxies in the list. When a redundant Proxy is located, the device either continues operating with it until the next failure occurs or reverts to the primary Proxy (refer to the parameter ProxyRedundancyMode). If none of the Proxy servers respond, the device goes over the list again.</p> <p>The device also provides real-time switching (Hot-Swap mode) between the primary and redundant proxies (refer to the parameter IsProxyHotSwap). If the first Proxy doesn't respond to the INVITE message, the same INVITE message is immediately sent to the next Proxy in the list. The same logic applies to REGISTER messages (if RegistrarIP is not defined).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 ProxyDNSQueryType is set to 1 or 2.
Transport Type [ProxyIp_TransportType]	<p>The transport type per Proxy server.</p> <ul style="list-style-type: none"> ▪ [0] UDP ▪ [1] TCP ▪ [2] TLS ▪ [-1] = Undefined <p>Note: If no transport type is selected, the value of the global parameter SIPTransportType is used (see 'Configuring SIP General Parameters' on page 221).</p>
Web/EMS: Enable Proxy Keep Alive [ProxySet_EnableProxyKeepAlive]	<p>Determines whether Keep-Alive with the Proxy is enabled or disabled. This parameter is configured per Proxy Set.</p> <ul style="list-style-type: none"> ▪ [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

Parameter	Description
	<p>REGISTER messages.</p> <p>If set to 'Using Options', the SIP OPTIONS message is sent every user-defined interval (configured by the parameter ProxyKeepAliveTime). If set to 'Using Register', the SIP REGISTER message is sent every user-defined interval (configured by the RegistrationTime parameter). Any response from the Proxy, either success (200 OK) or failure (4xx response) is considered as if the Proxy is communicating correctly.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For Survivability mode for USER-type IP Groups, this parameter must be enabled (1 or 2). ▪ 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.
<p>Web: Proxy Keep Alive Time EMS: Keep Alive Time [ProxySet_ProxyKeepAliveTime]</p>	<p>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.</p> <p>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.</p>
<p>Web: Proxy Load Balancing Method EMS: Load Balancing Method [ProxySet_ProxyLoadBalancingMethod]</p>	<p>Enables the Proxy Load Balancing mechanism per Proxy Set ID.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Load Balancing is disabled (default) ▪ [1] Round Robin ▪ [2] Random Weights <p>When the Round Robin algorithm is used, a list of all possible Proxy IP addresses is compiled. This list includes all IP addresses per Proxy Set, after necessary DNS resolutions (including NAPTR and SRV, if configured). After this list is compiled, the Proxy Keep-Alive mechanism (according to parameters EnableProxyKeepAlive and ProxyKeepAliveTime) tags each entry as 'offline' or 'online'. Load balancing is only performed on Proxy servers that are tagged as 'online'.</p> <p>All outgoing messages are equally distributed across the list of IP addresses. REGISTER messages are also distributed unless a RegistrarIP is configured.</p> <p>The IP addresses list is refreshed according to ProxyIPListRefreshTime. If a change in the order of the entries in the list occurs, all load statistics are erased and balancing starts over again.</p> <p>When the Random Weights algorithm is used, the outgoing requests are not distributed equally among the Proxies. The weights are received from the DNS server by using SRV records. The device sends the requests in such a fashion that each Proxy receives a percentage of the requests according to its' assigned weight. A single</p>

Parameter	Description
	<p>FQDN should be configured as a Proxy IP address. The Random Weights Load Balancing is not used in the following scenarios:</p> <ul style="list-style-type: none"> 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]	<p>Enables the Proxy Hot-Swap redundancy mode per Proxy Set.</p> <ul style="list-style-type: none"> [0] No (default) [1] Yes <p>If Proxy Hot-Swap is enabled, the SIP INVITE/REGISTER message is initially sent to the first Proxy/Registrar server. If there is no response from the first Proxy/Registrar server after a specific number of retransmissions (configured by the parameter HotSwapRtx), the message is resent to the next redundant Proxy/Registrar server.</p>
Web/EMS: Redundancy Mode [ProxySet_ProxyRedundancyMode]	<p>Determines whether the device switches back to the primary Proxy after using a redundant Proxy (per this Proxy Set).</p> <ul style="list-style-type: none"> [-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). <p>Notes:</p> <ul style="list-style-type: none"> 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.
Web/EMS: SRD Index [ProxySet_ProxySet_SRD]	<p>The SRD (defined in Configuring SRD Table on page 189) associated with the Proxy Set ID.</p> <p>Notes:</p> <ul style="list-style-type: none"> For this parameter to take effect, a device reset is required. If no SRD is defined for this parameter, by default, SRD ID #0 is associated with the Proxy Set.

14.5 Configuring NAT Translation per IP Interface

The NAT Translation table defines NAT rules for translating source IP addresses per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses (*global*). This allows, for example, the separation of VoIP traffic between different ISTP's, and topology hiding of internal IP addresses to the “public” network. Each IP interface (configured in the Multiple Interface table - InterfaceTable parameter) can be associated with a NAT rule in this table, translating the source IP address and port of the outgoing packet into the NAT address (IP address and port range).

The device's priority method for performing NAT is as follows:

- a. Uses an external STUN server (STUNServerPrimaryIP parameter) to assign a NAT address to all interfaces.

- b. Uses the StaticNATIP parameter to define one NAT IP address for all interfaces.
- c. Uses the NATTranslation parameter to define NAT per interface.

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

➤ **To configure NAT translation rules:**

1. Open the NAT Translation Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **NAT Translation Table**).

Figure 14-2: NAT Translation Table Page

Index	Source Interface Name	Target IP Address	Source Start Port	Source End Port	Target Start Port	Target End Port
1	voice	107.20.22.10				

2. Configure the parameters according to the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

Table 14-5: NAT Translation Table Parameters

Parameter	Description
Index [NATTranslation_Index]	Defines the table index entry. This table can include up to 32 entries.
Source Interface Name [NATTranslation_SourceInterfaceName]	Defines the name of the IP interface, as appears in the Multiple Interface table. Note: If the Multiple Interface table is not configured, the default Source IP Interface Name is "All". This represents the single IP interface for OAMP, Control, and Media (defined by the LocalOAMIPAddress, LocalOAMSubnetMask, and LocalOAMDefaultGW parameters).
Target IP Address [NATTranslation_TargetIPAddress]	Defines the global IP address.
Source Start Port [NATTranslation_SourceStartPort]	Defines the optional starting port range (1-65536) of the global address. If no ports are required, leave this field blank.
Source End Port [NATTranslation_SourceEndPort]	Defines the optional ending port range (1-65536) of the global address. If no ports are required, leave this field blank.
Target Start Port [NATTranslation_TargetStartPort]	Defines the optional starting port range (1-65536) of the IP interface. If no ports are required, leave this field blank.
Target End Port [NATTranslation_TargetEndPort]	Defines the optional ending port range (1-65536) of the IP interface. If no ports are required, leave this field blank.

14.6 Multiple SIP Signaling and Media Interfaces using SRDs

The device supports the configuration of multiple, logical SIP signaling interfaces and media (RTP) interfaces. Multiple SIP and media interfaces allows you to:

- Separate SIP and media traffic between different applications (i.e., SAS, Gateway\IP-to-IP)
- Separate SIP and media traffic between different Layer-3 networks (e.g., when operating with multiple ITSPs - separation of signaling traffic between different customers). This separation allows you to use different routing rules, manipulations, SIP definitions, etc. per network (customer). This is also applicable for networks residing in the same or in different Layer-3 networks as the device. In such a scenario, the device is configured with multiple SRDs.
- Implement different SIP signaling ports (listening UDP, TCP, and TLS, and the UDP source ports) for single or multiple interfaces.
- Only one signaling interface per application type is allowed per SRD. An SRD can be associated with many SIP interfaces which are based on one Layer-3 interface, with different ports.

Multiple SIP and RTP interfaces are implemented using SRDs (Signaling Routing Domains). An SRD is a set of definitions of IP interfaces, device resources, SIP behaviors and other definitions that together create (from the IP user's perspective), multiple, virtual multi-service gateways, from one physical device.

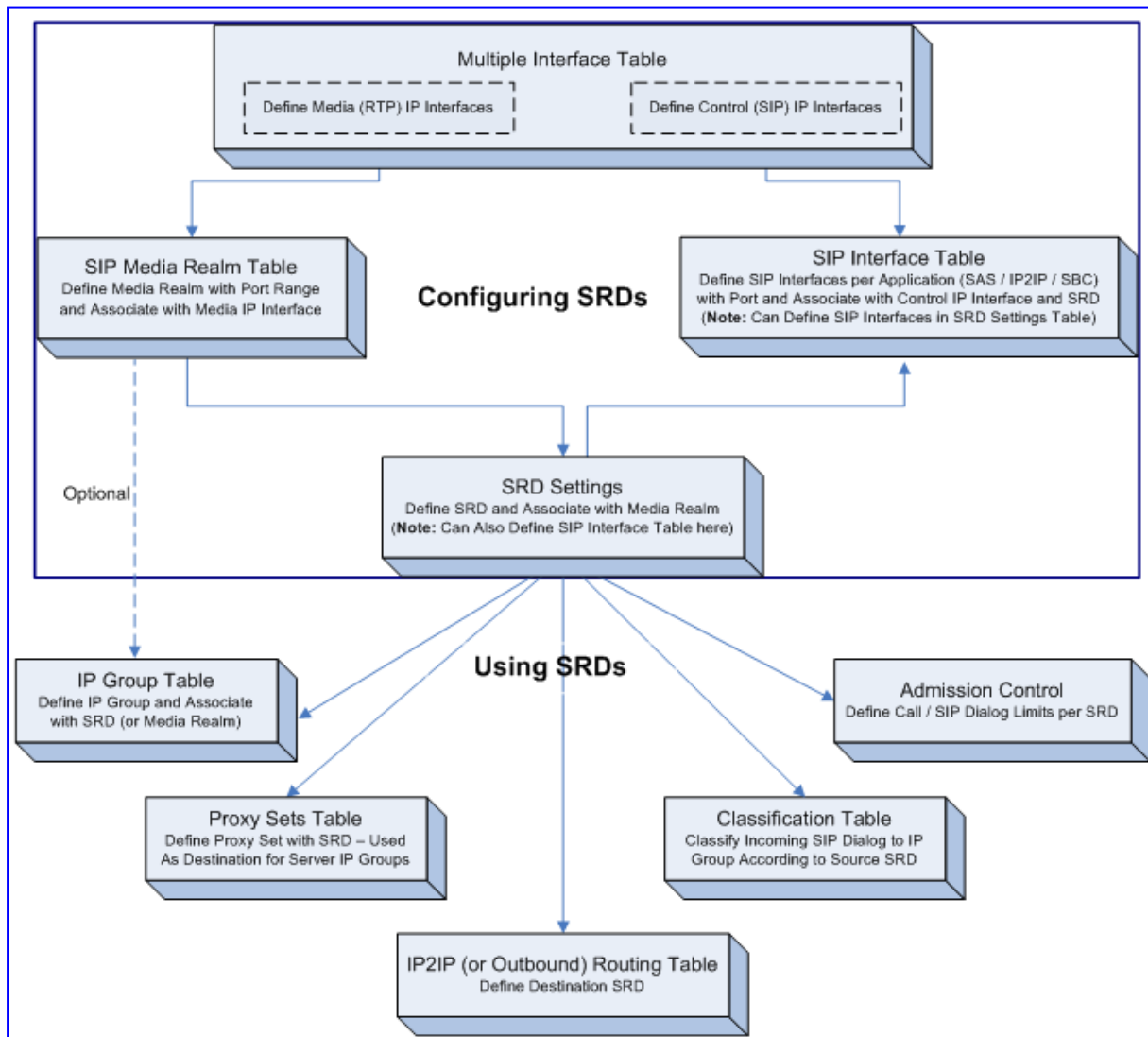
An SRD is composed of the following main entities:

- **Media Realm:** A Media Realm is a range of UDP ports associated with a specific Media-type IP interface (defined in the Multiple Interface table in 'Configuring IP Interface Settings' on page 102). You can configure multiple Media Realms (each with a specified UDP port range) for a specific media IP interface, thereby allowing you to divide a media IP interface (RTP traffic) into a pool of media realms. Media Realms are configured in the Media Realm table (see 'Configuring Media Realms' on page 170). Once configured, you can assign Media Realms to an SRDs (and/or IP Groups).
- **SIP Interface:** A SIP Interface is a combination of UDP, TCP, and/or TLS ports associated with a specific Control-type IP interface (defined in the Multiple Interface table). Therefore, a SIP Interface represents a SIP signaling interface. SIP Interfaces are configured in the SIP Interface table (see 'Configuring SIP Interface Table' on page 191) where they are assigned to SRDs:
 - Each SIP Interface is defined with a unique signaling port (i.e., no two SIP Interfaces can share the same port - no overlapping).
 - SIP Interfaces assigned to a specific SRD ID must all be defined with the same network interface (from the Multiple Interface table). For example, if you define three SIP Interfaces for SRD ID #8, all these SIP Interfaces must be defined with the same network interface (e.g., "SIP1").
 - Each SIP Interface assigned to a specific SRD ID must be defined with a different application type (i.e., SAS, Gateway\IP-to-IP). Therefore, up to two SIP Interfaces can be assigned to a specific SRD.

Once configured, you can use an SRD as follows:

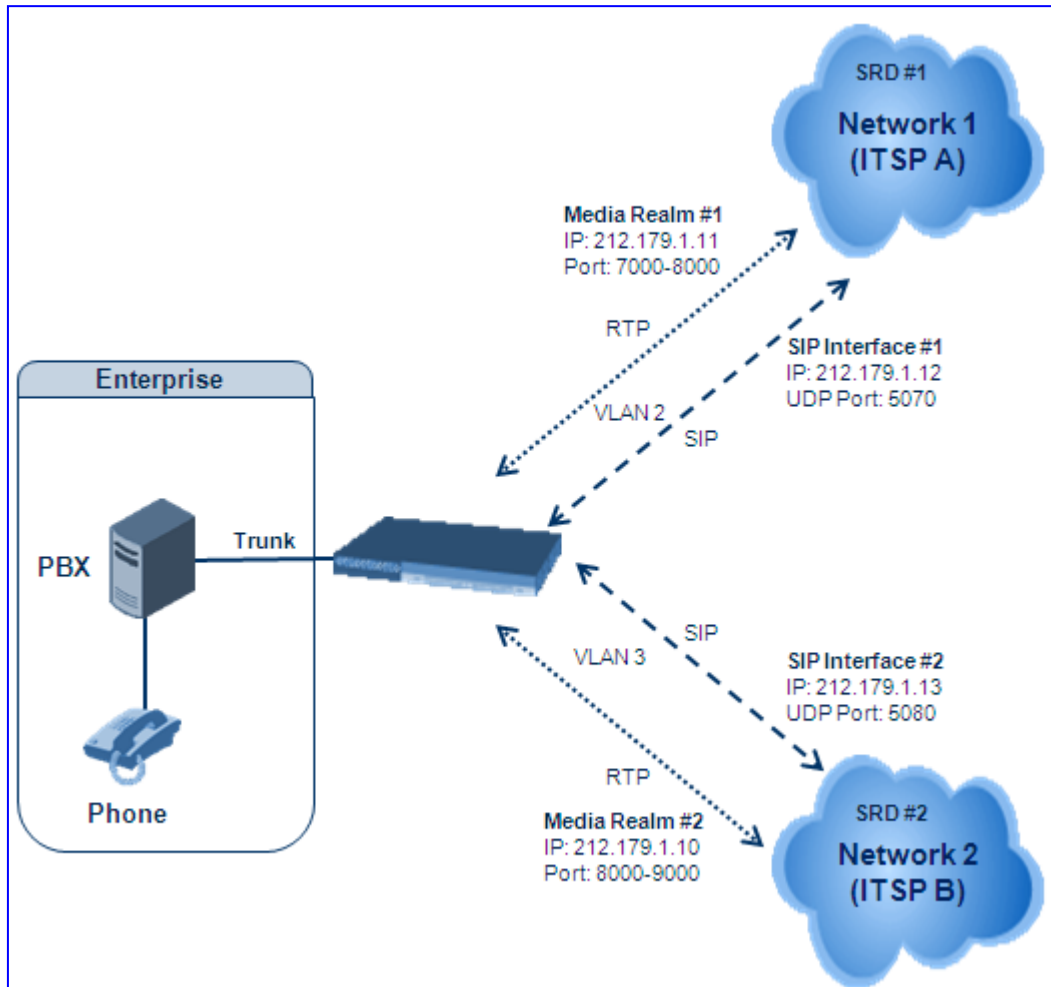
- Associate it with an IP Group (see Configuring IP Groups on page 193).
- Associate it with a Proxy Set (see Configuring Proxy Sets Table on page 198).
- Define it as a destination SRD for IP-to-IP routing rules (see Configuring IP-to-IP Routing Table). Routing from one SRD to another is possible, where each routing destination (IP Group or destination address) indicates the SRD to which it belongs.

Figure 14-3: Configuring SRDs and Assignment



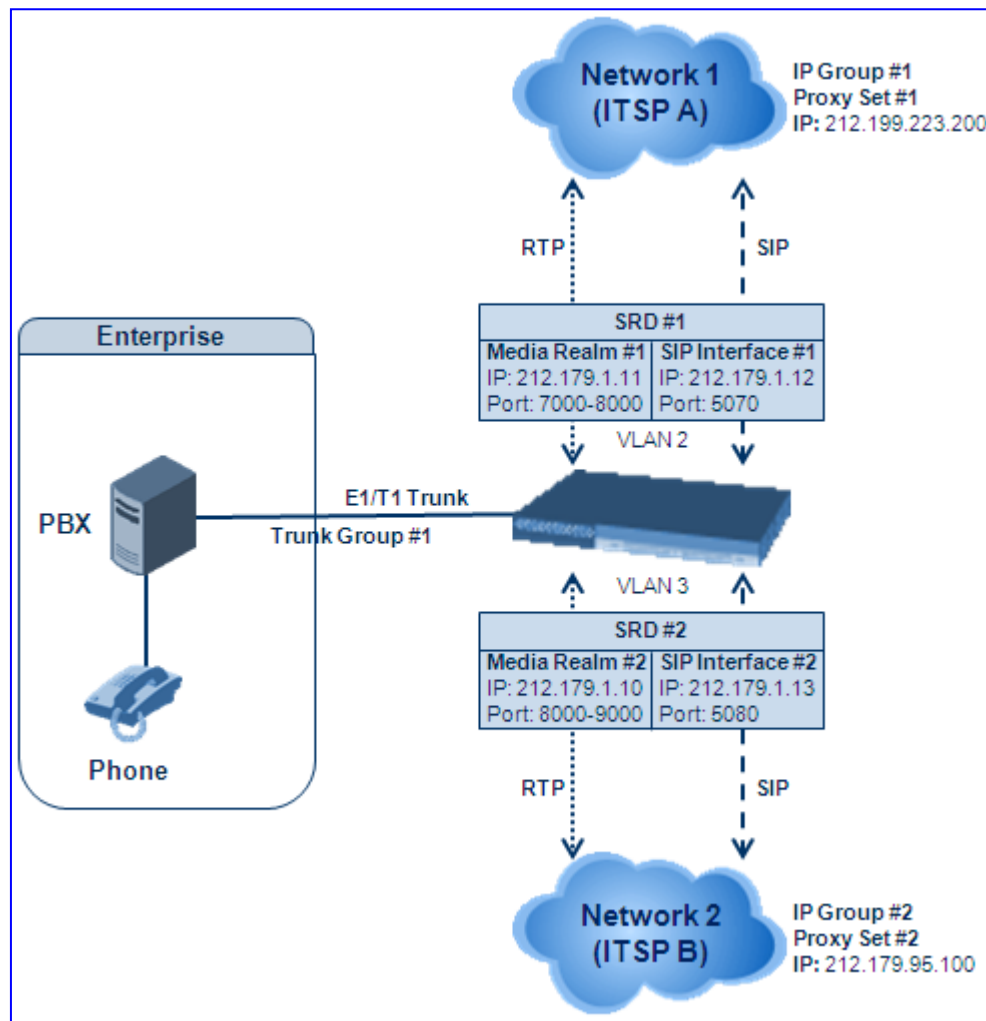
Typically, an SRD is defined per group of SIP UAs (e.g., proxies, IP phones, application servers, gateways, softswitches) that communicate with each other. This provides these entities with VoIP services that reside on the same Layer-3 network (must be able to communicate without traversing NAT devices and must not have overlapping IP addresses).

The figure below illustrates a typical scenario for implementing multiple SIP signaling interfaces. In this example, different SIP signaling interfaces and RTP traffic interfaces are assigned to Network 1 (ITSP A) and Network 2 (ITSP B).



Below provides an example for configuring multiple SIP signaling and RTP interfaces. In this example, the device serves as the interface between the enterprise's PBX (connected using an E1/T1 trunk) and two ITSP's, as shown in the figure below:

Figure 14-4: Multiple SIP Signaling/RTP Interfaces Example



Note that only the steps specific to multiple SIP signaling/RTP configuration are described in detail in the procedure below.

➤ **To configure multiple SIP signaling and RTP interfaces:**

1. Configure Trunk Group ID #1 in the Trunk Group Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Trunk Group** > **Trunk Group**), as shown in the figure below:

Add Phone Context As Prefix		Disable	
Trunk Group Index		1-12	

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 PRI	1	1	1-31	1000	1	
2							

2. Configure the trunk in the Trunk Settings page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Trunk Group** > **Trunk Group Settings**).
3. Configure the IP interfaces in the Multiple Interface table (**Configuration** tab > **VoIP** menu > **Network** submenu > **IP Settings**):

Figure 14-5: Defining IP Interfaces (Only Relevant Fields are Shown)

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	DAMP + Media + Control	192.168.0.2	24	192.168.0.1	1	Voice
1	Media	212.179.1.11	16	0.0.0.0	2	Media1
2	Media	212.179.1.10	16	0.0.0.0	3	Media2
3	Control	212.179.1.12	16	0.0.0.0	2	SIP1
4	Control	212.179.1.13	16	0.0.0.0	3	SIP2

4. Configure Media Realms in the Media Realm table (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Realm Configuration**):

Figure 14-6: Defining Media Realms

Index	Media Realm Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End
1	Realm1	Media1	7000	101	8000
2	Realm2	Media2	8020	20	8210

5. Configure SRDs in the SRD table (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SRD Table**):
 - SRD1 associated with media realm "Realm1".
 - SRD2 associated with media realm "Realm2".

Figure 14-7: Defining SRDs

SRD Index	0 - SRD1
Common Parameters	
SRD Name	SRD1
Media Realm	Realm1
SBC Parameters	
IP Group Status Table	Proxy Sets Status Table

6. Configure the SIP Interfaces in the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SIP Interface Table**):

Figure 14-8: Defining SIP Interfaces

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD
1	SIP1	Gw\IP2IP	5070	5070	5071	1
2	SIP2	Gw\IP2IP	5080	5080	5081	2

7. Configure Proxy Sets in the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**). The figure below configures ITSP A. Do the same for ITSP B but for Proxy Set 2 with IP address 212.179.95.100 and SRD 2.

Figure 14-9: Defining Proxy Set

Proxy Set ID		1
	Proxy Address	Transport Type
1	212.199.223.200	UDP
2		
3		
4		
5		
Enable Proxy Keep Alive		Disable
Proxy Keep Alive Time		60
Proxy Load Balancing Method		Disable
Is Proxy Hot Swap		No
Proxy Redundancy Mode		(-1) - Not Configured
SRD Index		1

- Configure IP Groups in the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **IP Group Table**). The figure below configures IP Group for ITSP A. Do the same for ITSP B but for Index 2 with SRD 1 and Media Realm to "Realm2".

Figure 14-10: Defining IP Groups

Index	1
Common Parameters	
Type	SERVER
Description	ITSP A
Proxy Set ID	1
SIP Group Name	
Contact User	
SRD	1
Media Realm	
IP Profile ID	1

- Configure IP-to-Trunk Group routing in the Inbound IP Routing Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** submenu > **IP to Trunk Group Routing**):

Figure 14-11: Defining IP-to-Trunk Group Routing

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID
1	*	*	*	*	*	1
2						

- Configure Trunk Group-to-IP routing in the Outbound IP Routing Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** submenu > **Tel to IP Routing**):

Figure 14-12: Defining Trunk Group to IP Group Routing

Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address	Port	Transport Type	Dest. IPGroup ID
1	[0-1]	*			Not Configured	1
1	*	*			Not Configured	2

15 Enabling Applications

The device supports the following main applications:

- Stand-Alone Survivability (SAS) application
- IP2IP application

The procedure below describes how to enable these applications. Once an application is enabled, the Web GUI provides menus and parameter fields relevant to the application.



Notes:

- This page displays the application only if the device is installed with the relevant Software Upgrade Key supporting the application (see 'Loading Software Upgrade Key' on page 485).
- The IP2IP application is applicable only to Mediant 1000.
- For configuring the SAS application, see 'Stand-Alone Survivability (SAS) Application' on page 371.
- For an overview of the IP2IP application and configuration examples, see IP-to-IP Routing Application on page 351.
- For enabling an application, a device reset is required.
- The Gateway and IP-to-IP applications are depicted in the Web interface as "GW" and "IP2IP" respectively.

➤ To enable an application:

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

⚡ Enable SAS	Disable	▼
⚡ Enable IP2IP Application	Disable	▼

2. Save the changes to the device's flash memory and then reset the device (see 'Saving Configuration' on page 470).

Reader's Notes

16 Coders and Profiles

This section describes configuration of the coders and SIP profiles parameters.

16.1 Configuring Coders

The Coders page allows you to configure up to 10 voice coders for the device to use. Each coder can be configured with packetization time (ptime), rate, payload type, and silence suppression.

The first coder in the table has the highest priority and is used by the device whenever possible. If the remote side cannot use the first coder, the device attempts to use the next coder in the table, and so on.



Notes:

- For a list of supported coders and for configuring coders using the *ini* file, refer to the *ini* file parameter table CodersGroup, described in 'Configuration Parameters Reference' on page 529.
- Each voice coder 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).
- For defining groups of coders, which can be assigned to Tel and IP Profiles, see 'Configuring Coder Groups' on page 214.
- For information on V.152 and implementation of T.38 and VBD coders, see 'Supporting V.152 Implementation' on page 150.



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

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

Figure 16-1: 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 **Submit** to apply your changes.
9. To save the changes to flash memory, see 'Saving Configuration' on page 470.

16.2 Configuring Coder Groups

The Coder Group Settings page allows you to define up to four groups of coders (termed *Coder Groups*). For each Coder Group, you can define up to 10 coders, configured with packetization time (ptime), rate, payload type, and silence suppression. The first coder in the Coder Group table is the highest priority coder and is used by the device whenever possible. If the remote side cannot use the first coder, the device attempts to use the next coder, and so on.

Coder Groups can be used as follows:

- Assigned to Tel Profiles in the Tel Profiles table (see *Configuring Tel Profiles* on page 215).
- Assigned to IP Profiles in the IP Profiles table (see *'Configuring IP Profiles'* on page 217).



Notes:

- Each voice coder 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 'Configuration Parameters Reference' on page 529.
- For information on coders, refer to the notes in 'Configuring Coders' on page 213.

➤ **To configure Coder Groups:**

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

Figure 16-2: Coder Group Settings Page

▼				
Coder Group ID		1 ▼		
Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.723.1 ▼	30 ▼	5.3 ▼	4	Disabled ▼
▼	▼	▼		▼
▼	▼	▼		▼
▼	▼	▼		▼
▼	▼	▼		▼

2. From the 'Coder Group ID' drop-down list, select a Coder Group ID.
3. From the 'Coder Name' drop-down list, select the first coder for the Coder Group.
4. From the 'Packetization Time' drop-down list, select the packetization time (in msec) for the coder. The packetization time determines how many coder payloads are combined into a single RTP packet.
5. From the 'Rate' drop-down list, select the bit rate (in kbps) for the coder you selected.
6. In the 'Payload Type' field, if the payload type (i.e., format of the RTP payload) for the coder you selected is dynamic, enter a value from 0 to 120 (payload types of '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 **Submit** to apply your changes.
11. To save the changes to flash memory, see 'Saving Configuration' on page 470.

16.3 Configuring Tel Profile

The Tel Profile Settings page allows you to define up to nine SIP profiles for Tel calls (termed *Tel Profiles*). Each Tel Profile contains a set of parameters for configuring various behaviors, for example, used coder, silence suppression support, and echo canceler. Once configured, Tel Profiles can then be assigned to specific trunks (channels). For example, specific channels can be assigned a Tel Profile that must use the G.711 coder. Thus, implementing Tel Profiles provides high-level adaptation when connected to a variety of equipment and protocols (at both Tel and IP sides), each of which may require different system behavior.

The Tel Profiles are assigned to the device's channels in the Trunk Group Table (see Configuring the Trunk Group Table on page 249)).



Note: You can also configure Tel Profiles using the *ini* file table parameter TelProfile (see 'Configuration Parameters Reference' on page 529).

➤ **To configure Tel Profiles:**

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

Profile ID	1
Profile Name	mike
▼ Profile Parameters	
Profile Preference	1
Fax Signaling Method	No Fax
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
RTP IP DiffServ	46
Signaling DiffServ	40
Voice Volume (-32 to 31 dB)	0
DTMF Volume (-31 to 0 dB)	-11
Input Gain (-32 to 31 dB)	0
Enable Digit Delivery	Disable
Enable Polarity Reversal	Enable
Enable Current Disconnect	Disable
MWI Analog Lamp	Disable
MWI Display	Disable
Dial Plan Index	-1
Echo Canceler	Enable
Flash Hook Period	700
Enable Early Media	Disable
Progress Indicator to IP	Not Configured
Enable DID Wink	Disable
Dialing Mode	Two Stages
Enable Voice Mail Delay	Enable
Disconnect Call on Detection of Busy Tone	Enable
Time For Reorder Tone [sec]	255
Enable 911 PSAP	Disable
Enable AGC	Disable
EC NLP Mode	Adaptive NLP
Swap Tel To IP Phone Numbers	Disable
▼ Coder Group	
Coder Group	Default Coder Group

2. From the 'Profile ID' drop-down list, select the Tel Profile index.
3. In the 'Profile Name' field, enter an arbitrary name that enables you to easily identify the Tel Profile.
4. From the 'Profile Preference' drop-down list, select the priority of the Tel Profile, where **1** is the lowest priority and **20** the highest. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk in the description of the parameter TelProfile) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.
Note: If the coder lists of both IP and Tel Profiles apply to the same call, only the

coders common to both are used. The order of the coders is determined by the preference.

5. Configure the parameters as required. For more 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 214) or the device's default coder (see 'Configuring Coders' on page 213) to which you want to assign the Tel Profile.
7. Click **Submit** to apply your changes.
8. To save the changes to flash memory, see 'Saving Configuration' on page 470.

16.4 Configuring IP Profiles

The IP Profile Settings page allows you to define up to nine SIP profiles for IP calls (termed *IP Profile*). Each IP Profile contains a set of parameters for configuring various behaviors, for example, used coder, echo canceller support, and jitter buffer. Once configured, different IP Profiles can be assigned to specific inbound and outbound calls. For example, specific calls can be assigned an IP Profile that must use the G.711 coder. Thus, implementing IP Profiles provides high-level adaptation when connected to a variety of equipment and protocols (at both Tel and IP sides), each of which may require different system behavior.

The IP Profiles can be used in the following tables:

- Outbound IP Routing Table - see 'Configuring Outbound IP Routing Table' on page 269
- Inbound IP Routing Table - see 'Configuring Inbound IP Routing Table' on page 277
- IP Group table - see 'Configuring IP Groups' on page 193

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 the GW (gateway) application



Notes:

- For a detailed description of each IP Profile 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 AlwaysUseRouteTable parameter is set to 1).
- You can use IP Profiles in the IP Group table, Outbound IP Routing table, and Inbound IP Routing table. The device selects the IP Profile as follows:
 - 1) If different IP Profiles (not default) are assigned to these tables, the device uses the IP Profile with the highest preference level (as set in the 'Profile Preference' field). If they have the same preference level, the device uses the IP Profile assigned to the IP Group table.
 - 2) If different IP Profiles are assigned to these tables and one table is set to the default IP Profile, the device uses the IP Profile that is not the default.
- You can also configure IP Profiles using the *ini* file table parameter IPProfile (see 'Configuration Parameters Reference' on page 529).

➤ **To configure IP Profiles:**

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

Profile ID	1
Profile Name	
Common Parameters	
RTP IP DiffServ	46
Signaling DiffServ	40
Disconnect on Broken Connection	Yes
Dynamic Jitter Buffer Minimum Delay [msec](*)	10
Dynamic Jitter Buffer Optimization Factor(*)	10
RTP Redundancy Depth(*)	0
Echo Canceler(*)	Enable
Input Gain (-32 to 31 dB)(*)	0
Voice Volume (-32 to 31 dB)(*)	0
Gateway Parameters	
Fax Signaling Method	No Fax
Play Ringback Tone to IP	Don't Play
Enable Early Media	Disable
Copy Destination Number to Redirect Number	Disable
Media Security Behavior	Preferable
CNG Detector Mode	Disable
Modems Transport Type	Enable Bypass
NSE Mode	Disable
Number of Calls Limit	-1
Progress Indicator to IP	Not Configured
Profile Preference	1
Coder Group	Default Coder Group
Remote RTP Base UDP Port	0
First Tx DTMF Option	RFC 2833
Second Tx DTMF Option	
Declare RFC 2833 in SDP	Yes
Add IE In SETUP	
AMD Sensitivity Parameter Suit	0
AMD Sensitivity Level	8
AMD Max Greeting Time	300
AMD Max Post Silence Greeting Time	400
Enable Hold	Enable

2. From the 'Profile ID' drop-down list, select the IP Profile index.
3. In the 'Profile Name' field, enter an arbitrary name that allows you to easily identify the IP Profile.

4. From the 'Profile Preference' drop-down list, select the priority of the IP Profile, where '1' is the lowest priority and '20' is the highest. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.
Note: If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used. The order of the coders is determined by the preference.
5. Configure the parameters as required.
6. 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 213), or one of the coder groups you defined in the Coder Group Settings page (see 'Configuring Coder Groups' on page 214).
7. Click **Submit** to apply your changes.
8. To save the changes to flash memory, see 'Saving Configuration' on page 470.

Reader's Notes

17 SIP Definitions

This section describes configuration of SIP parameters.

17.1 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 529.

➤ **To configure general SIP parameters:**

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

SIP General	
NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Disable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disable
Fax Signaling Method	No Fax
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	UDP
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPs	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5060
Use user=phone in SIP URL	Yes
Use user=phone in From Header	No
Use Tel URI for Asserted Identity	Disable
Tel to IP No Answer Timeout	180
Enable Remote Party ID	Disable
Add Number Plan and Type to RPI Header	Yes
Enable History-Info Header	Disable
Use Source Number as Display Name	No
Use Display Name as Source Number	No
Enable Contact Restriction	Disable
Play Ringback Tone to IP	Don't Play
Play Ringback Tone to Tel	Prefer IP
Use Tgrp information	Disable
Enable GRUU	Disable
User-Agent Information	
SDP Session Owner	AudiocodesGW
Play Busy Tone to Tel	Don't Play
Subject	
Multiple Packetization Time Format	None
Enable Semi-Attended Transfer	Disable
3xx Behavior	Forward
Enable P-Charging Vector	Disable
Enable VoiceMail URI	Disable
Retry-After Time	0
Enable P-Associated-URI Header	Disable
Source Number Preference	
Forking Handling Mode	Parallel handling
Enable Comfort Tone	Disable
Add Trunk Group ID as Prefix to Source	No
Fake Retry After	0
Enable Reason Header	Enable
Retransmission Parameters	
SIP T1 Retransmission Timer [msec]	500
SIP T2 Retransmission Timer [msec]	4000
SIP Maximum RTX	7

2. Configure the parameters as required.

3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

17.2 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 529.

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

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

General	
IP Security	Disable
Filter Calls to IP	Don't Filter
Enable Digit Delivery to Tel	Disable
Enable Digit Delivery to IP	Disable
Enable DID Wink	Disable
Delay Before DID Wink	0
Reanswer Time	0
PSTN Alert Timeout	180
QoS Statistics in SIP Release Call	Disable
Disconnect and Answer Supervision	
Send Digit Pattern on Connect	
Enable Polarity Reversal	Disable
Enable Current Disconnect	Disable
Disconnect on Broken Connection	Yes
Broken Connection Timeout [100 msec]	100
Disconnect Call on Silence Detection	No
Silence Detection Period [sec]	120
Silence Detection Method	Voice/Energy Detectors
Enable Fax Re-Routing	Disable
CDR and Debug	
CDR Server IP Address	
CDR Report Level	None
Misc. Parameters	
Progress Indicator to IP	Not Configured
Enable Busy Out	Disable
Graceful Busy Out Timeout [sec]	0
Default Release Cause	3
Max Number of Active Calls	200
Max Call Duration [min]	0
Enable LAN Watchdog	Disable
Enable Calls Cut Through	Disable
Enable User-Information Usage	Disable
Out-Of-Service Behavior	1 Reorder Tone
Delay After Reset [sec]	7
T38 Fax Max Buffer	3000
Enable Microsoft Extension	Disable
Reliable Connection Persistent Mode	Disable
First Call Ringback Tone ID	-1
Call Pickup Key	
Enable Delayed Offer	Disable
Replace Number Sign With Escape Char	Disable
Enable Single DSP Transcoding	Disable
Enable Network ISDN Transfer	Enable
AMD Beep Detection Mode	Disabled
Source Header For Called Number	use RequestURI header
Add empty authorization header	Disable
IP2IP Registration Time	0
Tel2IP Call Forking Mode	Disable
Emergency Calls	
Emergency Numbers	
[min] Emergency Calls Regret Timeout	10
MS LDAP Settings	
MS LDAP OCS Number attribute name	msRTCSIP-PrimaryUserAddress
MS LDAP PBX Number attribute name	telephoneNumber
MS LDAP MOBILE Number attribute name	mobile

2. Configure the parameters as required.

3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

17.3 Configuring Account Table

The Account Table page allows you to define up to 32 *Accounts* per Trunk Group (*Served Trunk Group*) or source IP Group (*Served IP Group*). This is used 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 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 198) associated with these Serving IP Groups. A Trunk Group or source IP 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 Trunk Group or Served IP Group, but with different Serving IP Groups, user name/password, host name, and contact user values.

When using the Account table to register a Trunk Group (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 509.
- You can also configure the Account table using the *ini* file table parameter Account (see 'Configuration Parameters Reference' on page 529).

➤ To configure Accounts:

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

Figure 17-1: Account Table Page

Index	Served Trunk Group	Served IP Group	Serving IP Group	Username	Password	Host Name	Register	ContactUser
1	1	3	1	itpa	*	regona	Yes	ITSPA.A
2	1	2	2	itpb		regonb	No	TSPB

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 470.
6. To perform registration, click the **Register** button; to unregister, click **Unregister**. The registration method for each Trunk Group is according to the setting of the 'Registration Mode' parameter in the Trunk Group Settings page.



Note: For a description of the Web interface's table command buttons (e.g., **Duplicate** and **Delete**), see 'Working with Tables' on page 44.

Table 17-1: Account Table Parameters Description

Parameter	Description
Served Trunk Group [Account_ServedTrunkGroup]	<p>The Trunk 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 Trunk Group is the source Trunk Group from where the call originated. For IP-to-Tel calls, the Served Trunk Group is the 'Trunk Group ID' defined in the Inbound IP Routing Table' (see 'Configuring the Inbound IP Routing Table' on page 277). For defining Trunk Groups, see Configuring the Trunk Group Table on page 249.</p> <p>Note: For the IP2IP application, this parameter must be set to -1 (i.e., no trunk).</p>
Served IP Group [Account_ServedIPGroup]	<p>The Source IP Group (e.g., IP-PBX) for which registration and/or authentication is performed.</p> <p>Note: This field is applicable only when the IP2IP application is enabled.</p>
Serving IP Group [Account_ServingIPGroup]	<p>The destination IP Group ID (defined in 'Configuring IP Groups' on page 193) 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 198) associated with the IP Group. This occurs only in the following conditions:</p> <ul style="list-style-type: none"> ▪ The parameter 'Registration Mode' is set to 'Per Account' in the Trunk Group Settings table (see 'Configuring Trunk Group Settings' on page 251). ▪ The parameter 'Register' in this table is set to 1. <p>In addition, for a SIP call that is identified by both the Served Trunk Group/Served IP Group and Serving IP Group, the username and password for digest authentication defined in this table is used.</p> <p>For Tel-to-IP calls, the Serving IP Group is the destination IP Group defined in the Trunk Group Settings table or Outbound IP Routing Table (see 'Configuring the Outbound IP Routing Table' on page 269). For IP-to-Tel calls, the Serving IP Group is the 'Source IP Group ID' defined in the Inbound IP Routing Table (see 'Configuring the Inbound IP Routing Table' on page 277).</p> <p>Note: If no match is found in this table for incoming or outgoing calls, the username and password defined in the Authentication table for FXS interfaces (see Configuring Authentication on page 316) or by the global parameters UserName and Password (in the 'Proxy & Registration page) are used.</p>
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

Parameter	Description
	<p>Group' table is used instead. This parameter can be up to 49 characters.</p>
<p>Register [Account_Register]</p>	<p>Enables registration.</p> <ul style="list-style-type: none"> ▪ [0] No = Don't register ▪ [1] Yes = Enables registration <p>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 Trunk Group Settings table for the specific Trunk 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:</p> <pre style="background-color: #f0f0f0; padding: 5px;">REGISTER sip:xyz SIP/2.0 Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac1397582418 From: <sip:ContactUser@HostName>;tag=1c1397576231 To: <sip: ContactUser@HostName > Call-ID: 1397568957261200022256@10.33.37.78 CSeq: 1 REGISTER Contact: <sip:ContactUser@10.33.37.78>;expires=3600 Expires: 3600 User-Agent: Sip-Gateway/v.6.00A.008.002 Content-Length: 0</pre> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The Trunk Group account registration is not affected by the parameter IsRegisterNeeded. ▪ For the IP2IP application, you can configure this table so that a specific IP Group can register to multiple ITSP's. This is performed by defining several rows in this table containing the same Served IP Group, but with different Serving IP Groups, user/password, Host Name and Contact User parameters. ▪ If registration to an IP Group(s) fails for all the accounts defined in this table for a specific Trunk Group, and if this Trunk Group includes all the channels in the Trunk Group, the Trunk Group is set to Out-Of-Service if the parameter OOSOnRegistrationFail is set to 1 (see 'Proxy & Registration Parameters' on page 226).
<p>Contact User [Account_ContactUser]</p>	<p>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 in the IP Group Table page is used instead.</p> <p>Note: If registration fails, then the user part in the INVITE Contact header contains the source party number.</p>
<p>Application Type [Account_ApplicationType]</p>	<p>Note: This parameter is not applicable.</p>

17.4 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 529.




Note: To view whether the device or its endpoints have registered to a SIP Registrar/Proxy server, see Viewing Registration Status on page 509.

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

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

Use Default Proxy	Yes	▼
Proxy Set Table		
Proxy Name	<input type="text"/>	
Redundancy Mode	Parking	▼
Proxy IP List Refresh Time	60	
Enable Fallback to Routing Table	Disable	▼
Prefer Routing Table	No	▼
Use Routing Table for Host Names and Profiles	Disable	▼
Always Use Proxy	Disable	▼
Redundant Routing Mode	Routing Table	▼
SIP ReRouting Mode	Standard Mode	▼
Enable Registration	Disable	▼
Gateway Name	<input type="text"/>	
Gateway Registration Name	<input type="text"/>	
DNS Query Type	A-Record	▼
Proxy DNS Query Type	A-Record	▼
Subscription Mode	Per Endpoint	▼
Number of RTX Before Hot-Swap	3	
Use Gateway Name for OPTIONS	No	▼
User Name	joe	
Password	mikey	
Cnonce	Default_Cnonce	
Registration Mode	Per Endpoint	▼
Set Out-Of-Service On Registration Failure	Disable	▼
Challenge Caching Mode	None	▼
Mutual Authentication Mode	Optional	▼

2. Configure the parameters as required.
3. Click **Submit to** apply your changes.
4. Click the **Register** or **Un-Register** buttons to save your changes and register/unregister the device to a Proxy/Registrar. Instead of registering the entire device, you can register specific entities (FXS/FXO endpoints, Trunk Groups, BRI endpoints, and Accounts), by using the **Register** button located on the page in which these entities are configured.
5. To save the changes to flash memory, see 'Saving Configuration' on page 470.

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 198 for a description of this page).

Reader's Notes

18 GW and IP to IP

This section describes configuration for the GW/IP2IP applications.



Note: The "GW" and "IP2IP" applications refer to the Gateway and IP-to-IP applications respectively.

18.1 Digital PSTN

This section describes configuration of the public switched telephone network (PSTN) parameters.

18.1.1 Configuring TDM Bus Settings

The TDM Bus Settings page allows you to configure the device's Time-Division Multiplexing (TDM) bus settings. For a description of these parameters, see 'Configuration Parameters Reference' on page 529.

➤ **To configure the TDM Bus settings:**

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

PCM Law Select	MuLaw	▼
TDM Bus Clock Source	Internal	▼
TDM Bus PSTN Auto FallBack Clock	Disable	▼
TDM Bus PSTN Auto Clock Reverting	Disable	▼
Idle PCM Pattern	255	
Idle ABCD Pattern	0x0F	▼
TDM Bus Local Reference	1	
TDM Bus Type	Frainers	▼

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. Save the changes to flash memory (see 'Saving Configuration' on page 470).

18.1.2 Configuring CAS State Machines

The CAS State Machine page allows you to modify various timers and other basic parameters to define the initialization of the CAS state machine without changing the state machine itself (no compilation is required). The change doesn't affect the state machine itself, but rather the configuration.

The CAS table used can be chosen in two ways (using the parameter CasChannelIndex):

- Single CAS table per trunk
- Different CAS table per group of B-Channels in a trunk

➤ To modify the CAS state machine parameters:

1. Open the CAS State Machine page (**Configuration** tab > **VoIP** menu > **PSTN** submenu > **CAS State Machines**).

Figure 18-1: CAS State Machine Page

CAS Table Name	Generate Digit On Time	Generate Inter Digit Time	DTMF Max Detection Time	DTMF Min Detection Time	Max Incoming Address Digits	Max Incoming ANI Digits	Collect ANI	Digit Signaling System	Related Trunks
r2_mftable_korea_cp_delay300.dat	-1	-1	-1	-1	-1	-1	Default	Default	
r2_mftable_korea_cp_delay500.dat	-1	-1	-1	-1	-1	-1	Default	Default	

2. Ensure that the trunk is inactive. The trunk number displayed in the 'Related Trunks' field must be green. If it is red (indicating that the trunk is active), click the trunk number to open the Trunk Settings page (see 'Configuring Trunk Settings' on page 232), select the required Trunk number icon, and then click **Stop Trunk**.
3. In the CAS State Machine page, modify the required parameters according to the table below.
4. Once you have completed the configuration, activate the trunk if required in the Trunk Settings page, by clicking the trunk number in the 'Related Trunks' field, and in the Trunk Settings page, select the required Trunk number icon, and then click **Apply Trunk Settings**.
5. Click **Submit**, and then reset the device (see 'Resetting the Device' on page 467).

Notes:



- Don't modify the default values unless you fully understand the implications of the changes and know the default values. Every change affects the configuration of the state machine parameters and the call process related to the trunk you are using with this state machine.
- You can modify CAS state machine parameters only if the following conditions are met:
 - 1) Trunks are inactive (stopped), i.e., the 'Related Trunks' field displays the trunk number in green.
 - 2) State machine is not in use or is in reset, or when it is not related to any trunk. If it is related to a trunk, you must delete the trunk or deactivate (*Stop*) the trunk.
- Field values displaying '-1' indicate CAS default values. In other words, CAS state machine values are used.
- The modification of the CAS state machine occurs at the CAS application initialization only for non-default values (-1).
- For more information on the CAS Protocol table, refer to the *Product Reference Manual*.

Table 18-1: CAS State Machine Parameters Description


Parameter	Description
Generate Digit On Time [CasStateMachineGenerateDigitOnTime]	Generates digit on-time (in msec). The value must be a positive value. The default value is -1 (use value from CAS state machine).
Generate Inter Digit Time [CasStateMachineGenerateInterDigitTime]	Generates digit off-time (in msec). The value must be a positive value. The default value is -1 (use value from CAS state machine).



Parameter	Description
DTMF Max Detection Time [CasStateMachineDTMFMaxOnDetectionTime]	Detects digit maximum on time (according to DSP detection information event) in msec units. The value must be a positive value. The default value is -1 (use value from CAS state machine).
DTMF Min Detection Time [CasStateMachineDTMFMinOnDetectionTime]	Detects digit minimum on time (according to DSP detection information event) in msec units. The digit time length must be longer than this value to receive a detection. Any number may be used, but the value must be less than CasStateMachineDTMFMaxOnDetectionTime. The value must be a positive value. The default value is -1 (use value from CAS state machine).
MAX Incoming Address Digits [CasStateMachineMaxNumOfIncomingAddressDigits]	Defines the limitation for the maximum address digits that need to be collected. After reaching this number of digits, the collection of address digits is stopped. The value must be an integer. The default value is -1 (use value from CAS state machine).
MAX Incoming ANI Digits [CasStateMachineMaxNumOfIncomingANIDigits]	Defines the limitation for the maximum ANI digits that need to be collected. After reaching this number of digits, the collection of ANI digits is stopped. The value must be an integer. The default value is -1 (use value from CAS state machine).
Collet ANI [CasStateMachineCollectANI]	In some cases, when the state machine handles the ANI collection (not related to MFCR2), you can control the state machine to collect ANI or discard ANI. <ul style="list-style-type: none"> ▪ [0] No = Don't collect ANI. ▪ [1] Yes = Collect ANI. ▪ [-1] Default = Default value - use value from CAS state machine.
Digit Signaling System [CasStateMachineDigitSignalingSystem]	Defines which Signaling System to use in both directions (detection\generation). <ul style="list-style-type: none"> ▪ [0] DTMF = Uses DTMF signaling. ▪ [1] MF = Uses MF signaling (default). ▪ [-1] Default = Default value - use value from CAS state machine.

18.1.3 Configuring Trunk Settings

The Trunk Settings page allows you to configure the device's trunks. This includes selecting the PSTN protocol and configuring related parameters.

Some parameters can be configured when the trunk is in service, while others require you

to take the trunk out of service (by clicking the **Stop**  button). Once you have "stopped" a trunk, all calls are dropped and no new calls can be made on that trunk.

You can also deactivate a trunk (by clicking the **Deactivate**  button) for maintenance. Deactivation temporarily disconnects (logically) the trunk from the PSTN network. Upon trunk deactivation, the device generates an AIS alarm on that trunk to the far-end (as a result, an RAI alarm signal may be received by the device). A subsequent trunk activation (by clicking the **Activate**  button), reconnects the trunk to the PSTN network and clears the AIS alarm. Trunk deactivation is typically used for maintenance such as checking the trunk's physical integrity.

For a description of the trunk parameters, see 'PSTN Parameters' on page 670.



Notes:

- During trunk deactivation, trunk configuration cannot be performed.
- A stopped trunk cannot also be activated and a trunk cannot be deactivated if it has been stopped.

➤ To configure the trunks:

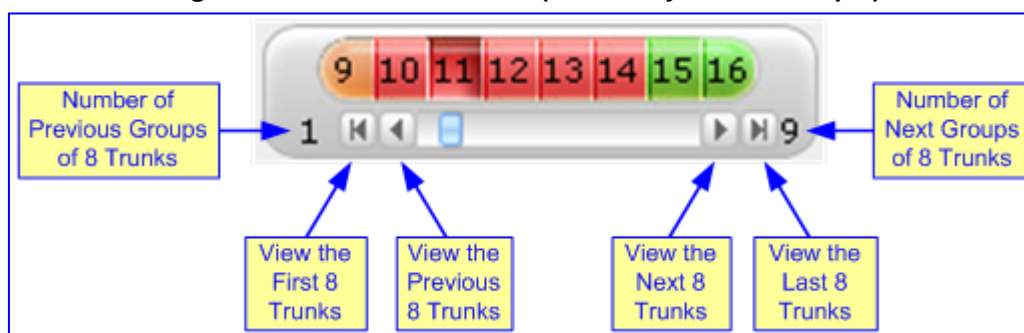
1. Open the Trunk Settings page (**Configuration** tab > **VoIP** menu > **PSTN** submenu > **Trunk Settings**).

General Settings	
Module ID	1
Trunk ID	1
Trunk Configuration State	Active
Protocol Type	T1 NI2 ISDN
Trunk Configuration	
Clock Master	Recovered
Auto Clock Trunk Priority	0
Line Code	B8ZS
Line Build Out Loss	0 dB
Trace Level	No Trace
Line Build Out Overwrite	OFF
Framing Method	T1 FRAMING ESF CRC6
ISDN Configuration	

On the top of the page, a bar with Trunk number icons displays the status of each trunk, according to the following color codes:




- **Grey:** Disabled
 - **Green:** Active
 - **Yellow:** RAI alarm (also appears when you deactivate a Trunk by clicking the **Deactivate** button)
 - **Red:** LOS/LOF alarm
 - **Blue:** AIS alarm
 - **Orange:** D-channel alarm (ISDN only)
2. Select the trunk that you want to configure by clicking the desired Trunk number icon. The bar initially displays the first eight trunk number icons (i.e., trunks 1 through 8). To scroll through the trunk number icons (i.e., view the next/last or previous/first group of eight trunks), refer to the figure below:

Figure 18-2: Trunk Scroll Bar (Used Only as an Example)



Note: If the Trunk scroll bar displays all available trunks, the scroll bar buttons are unavailable.

After you have selected a trunk, the following is displayed:

- The read-only 'Module ID' field displays the module number to which the trunk belongs.
 - The read-only 'Trunk ID' field displays the selected trunk number.
 - The read-only 'Trunk Configuration State' displays the state of the trunk ('Active' or 'Inactive').
 - The displayed parameters pertain to the selected trunk only.
3. Click the **Stop Trunk**  button (located at the bottom of the page) to take the trunk out of service so that you can configure the currently grayed out (unavailable) parameters. (Skip this step if you want to configure parameters that are available when the trunk is active). The stopped trunk is indicated by the following:
- The 'Trunk Configuration State' field displays 'Inactive'.
 - The **Stop Trunk** button is replaced by the **Apply Trunk Settings**  button.
- When all trunks are stopped, the **Apply to All Trunks**  button also appears.
- All the parameters are available and can be modified.
4. Configure the trunk parameters as required.

5. Click the **Apply Trunk Settings** button to apply the changes to the selected trunk (or click **Apply to All Trunks** to apply the changes to all trunks); the **Stop Trunk** button replaces **Apply Trunk Settings** and the 'Trunk Configuration State' displays 'Active'.
6. To save the changes to flash memory, see 'Saving Configuration' on page [470](#).
7. To reset the device, see 'Resetting the Device' on page [467](#).


Notes:

- If the 'Protocol Type' field displays 'NONE' (i.e., no protocol type is selected) and no other trunks have been configured, after selecting a PRI protocol type, you must reset the device.
- The displayed parameters depend on the protocol selected.
- All PRI trunks of the device must be of the same line type (i.e., E1 or T1). However, different variants of the same line type can be configured on different trunks, for example, E1 Euro ISDN and E1 CAS (subject to the constraints in the device's Release Notes).
- BRI trunks can operate with E1 or T1 trunks.
- If the protocol type is CAS, you can assign or modify a dial plan (in the 'Dial Plan' field) and perform this without stopping the trunk.
- If the trunk can't be stopped because it provides the device's clock (assuming the device is synchronized with the E1/T1 clock), assign a different E1/T1 trunk to provide the device's clock or enable 'TDM Bus PSTN Auto Clock' in the TDM Bus Settings page (see Configuring TDM Bus Settings on page [229](#)).
- To delete a previously configured trunk, set the parameter 'Protocol Type' to 'None'.

18.1.4 Configuring Digital Gateway Parameters

The Digital Gateway Parameters page allows you to configure miscellaneous digital parameters. For a description of these parameters, see 'Configuration Parameters Reference' on page 529.

➤ **To configure the digital gateway parameters:**

1. Open the Digital Gateway Parameters page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Digital Gateway** submenu > **Digital Gateway Parameters**).

Figure 18-3: Digital Gateway Parameters Page

B-channel Negotiation	Exclusive	▼
Swap Redirect and Called Numbers	No	▼
MFC R2 Category	1	
Disconnect Call on Busy Tone Detection (CAS)	Enable	▼
Disconnect Call on Busy Tone Detection (ISDN)	Disable	▼
⚡ Enable TDM Tunneling	Disable	▼
Send Screening Indicator to IP	Not Configured	▼
Send Screening Indicator to ISDN	Not Configured	▼
Add IE in SETUP		
Trunk Groups to Send IE		
Enable User-to-User IE for Tel to IP	Disable	▼
Enable User-to-User IE for IP to Tel	Disable	▼
Enable ISDN Tunneling Tel to IP	Disable	▼
Enable QSIG Tunneling	Disable	▼
Enable ISDN Tunneling IP to Tel	Disable	▼
ISDN Transfer on Connect	Alert	▼
Remove CLI when Restricted	No	▼
Remove Calling Name	Disable	▼
Tdm Over IP Minimum Calls For Trunk Activation	0	
ISDN Facility Trace	Disable	▼
Use EndPoint Number As Calling Number Tel2IP	Disable	▼
Use EndPoint Number As Calling Number IP2Tel	Disable	▼
Default Cause Mapping From ISDN to SIP	0	
Add Prefix to Redirect Number		
Copy Destination Number to Redirect Number	Don't copy	▼
Enable Calling Party Category	Disable	▼
ISDN SubAddress Format	ASCII	▼
Play Local RBT on ISDN Transfer	Don't play	▼
Send Local Time To ISDN Connect	Disable	▼
User To User Header Format	0	
⚡ Digital Out-Of-Service Behavior	Default	▼
Ignore BRI LOS Alarm	Enable	▼
MLPP		
MLPP Default Namespace	DSN	▼
Default Call Priority	0	
Preemption tone Duration	3	
RTP DSCP for MLPP Routine	-1	
RTP DSCP for MLPP Priority	-1	
RTP DSCP for MLPP Immediate	-1	
RTP DSCP for MLPP Flash	-1	
RTP DSCP for MLPP Flash-Override	-1	
RTP DSCP for MLPP Flash-Override-Override	-1	
MLPP Default Service Domain	000000	
MLPP Normalized Service Domain	000000	

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

18.1.5 Tunneling Applications

This section discusses the device's support for VoIP tunneling applications.

18.1.5.1 TDM Tunneling

The device's TDM Tunneling feature allows you to tunnel groups of digital trunk spans or timeslots (B-channels) over the IP network. TDM Tunneling utilizes the device's internal routing (without Proxy control) capabilities to receive voice and data streams from TDM (E1/T1/J1) spans or individual timeslots, convert them into packets, and then transmit them over the IP network (using point-to-point or point-to-multipoint device distributions). A device opposite it (or several devices when point-to-multipoint distribution is used) converts the IP packets back into TDM traffic. Each timeslot can be targeted to any other timeslot within a trunk in the opposite device.

When TDM Tunneling is enabled (the parameter `EnableTDMoverIP` is set to '1') on the originating device, the originating device automatically initiates SIP calls from all enabled B-channels belonging to the E1/T1/J1 spans that are configured with the protocol type 'Transparent' (for ISDN trunks) or 'Raw CAS' (for CAS trunks). The called number of each call is the internal phone number of the B-channel from where the call originates. The 'Inbound IP Routing Table' is used to define the destination IP address of the terminating device. The terminating device automatically answers these calls if its E1/T1 protocol type is set to 'Transparent' (`ProtocolType = 5`) or 'Raw CAS' (`ProtocolType = 3` for T1 and `9` for E1) and the parameter `ChannelSelectMode` is set to `0` (By Phone Number).



Note: It's possible to configure both devices to also operate in symmetric mode. To do so, set `EnableTDMoverIP` to `1` and configure the 'Outbound IP Routing Table' in both devices. In this mode, each device (after it's reset) initiates calls to the second device. The first call for each B-channel is answered by the second device.

The device continuously monitors the established connections. If for some reason, one or more calls are released, the device automatically re-establishes these 'broken' connections. In addition, when a failure in a physical trunk or in the IP network occurs, the device re-establishes the tunneling connections when the network is restored.



Note: It's recommended to use the keep-alive mechanism for each connection, by activating the 'session expires' timeout and using Re-INVITE messages.

The device supports the configuration (`TDMoIPInitiateInviteTime` and `TDMoIPInviteRetryTime` parameters) of the following timers for the TDM-over-IP tunneling application:

- Time between successive INVITEs sent from the same E1/T1 trunk.
- Time between call release and the new INVITE that is sent on the same channel. The call can be released if the device receives a 4xx or 5xx response.

By utilizing the 'Profiles' mechanism (see 'Coders and Profiles' on page 213), you can configure the TDM Tunneling feature to choose different settings based on a timeslot or groups of timeslots. For example, you can use low-bit-rate vocoders to transport voice and 'Transparent' coder to transport data (e.g., for D-channel). You can also use Profiles to assign ToS (for DiffServ) per source - a timeslot carrying data or signaling is assigned a higher priority value than a timeslot carrying voice.

For tunneling of E1/T1 CAS trunks, set the protocol type to 'Raw CAS' (`ProtocolType = 3 / 9`) and enable RFC 2833 CAS relay mode ('CAS Transport Type' parameter is set to 'CAS RFC2833 Relay').



Note: For TDM over IP, the parameter CallerIDTransportType must be set to '0' (disabled), i.e., transparent.

Below is an example of *ini* files for two devices implementing TDM Tunneling for four E1 spans. Note that in this example both devices are dedicated to TDM tunneling.

Terminating Side:

```

EnableTDMOverIP = 1
;E1_TRANSPARENT_31
ProtocolType_0 = 5
ProtocolType_1 = 5
ProtocolType_2 = 5
ProtocolType_3 = 5
[PREFIX]
PREFIX_DestinationPrefix, PREFIX_DestAddress, PREFIX_SourcePrefix,
PREFIX_ProfileId, PREFIX_MeteringCode, PREFIX_DestPort,
PREFIX_SrcIPGroupID, PREFIX_DestHostPrefix, PREFIX_DestIPGroupID,
PREFIX_SrcHostPrefix, PREFIX_TransportType,
PREFIX_SrcTrunkGroupID, PREFIX_DestSRD, PREFIX_CostGroup,
PREFIX_ForkingGroup;
Prefix 1 = *,10.8.24.12;
[\PREFIX]

;IP address of the device in the opposite
;location
;Channel selection by Phone number.
ChannelSelectMode = 0
;Profiles can be used do define different coders per B-channels
;such as Transparent
;coder for B-channels (timeslot 16) that carries PRI ;signaling.
[TrunkGroup]
FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum,
TrunkGroup_FirstTrunkId, TrunkGroup_LastTrunkId,
TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel,
TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId,
TrunkGroup_Module;
TrunkGroup 1 = 0,0,0,1,31,1000,1;
TrunkGroup 1 = 0,1,1,1,31,2000,1;
TrunkGroup 1 = 0,2,2,1,31,3000,1;
TrunkGroup 1 = 0,3,3,1,31,4000,1;
TrunkGroup 1 = 0,0,0,16,16,7000,2;
TrunkGroup 1 = 0,1,1,16,16,7001,2;
TrunkGroup 1 = 0,2,2,16,16,7002,2;
TrunkGroup 1 = 0,3,3,16,16,7003,2;
[/TrunkGroup]
[ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = g7231;
CodersGroup0 1 = Transparent;
[ \CodersGroup0 ]
[TelProfile]
FORMAT TelProfile_Index = TelProfile_ProfileName,
TelProfile_TelPreference, TelProfile_CodersGroupID,
TelProfile_IsFaxUsed, TelProfile_JitterBufMinDelay,

```

```

TelProfile_JitterBufOptFactor, TelProfile_IPDiffServ,
TelProfile_SigIPDiffServ, TelProfile_DtmfVolume,
TelProfile_InputGain, TelProfile_VoiceVolume,
TelProfile_EnableReversePolarity,
TelProfile_EnableCurrentDisconnect,
TelProfile_EnableDigitDelivery, TelProfile_EnableEC,
TelProfile_MWIAAnalog, TelProfile_MWIDisplay,
TelProfile_FlashHookPeriod, TelProfile_EnableEarlyMedia,
TelProfile_ProgressIndicator2IP;
TelProfile 1 = voice,$$,1,$$,,$$,,$$,,$$,,$$,,$$;
TelProfile 2 = data,$$,2,$$,,$$,,$$,,$$,,$$,,$$;
[\\TelProfile]
    
```

Originating Side:

```

;E1_TRANSPARENT_31
ProtocolType_0 = 5
ProtocolType_1 = 5
ProtocolType_2 = 5
ProtocolType_3 = 5
;Channel selection by Phone number.
ChannelSelectMode = 0
[TrunkGroup]
FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum,
TrunkGroup_FirstTrunkId, TrunkGroup_LastTrunkId,
TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel,
TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId,
TrunkGroup_Module;
TrunkGroup 0 = 0,0,0,1,31,1000,1;
TrunkGroup 0 = 0,1,1,1,31,2000,1;
TrunkGroup 0 = 0,2,2,1,31,3000,1;
TrunkGroup 0 = 0,3,1,31,4000,1;
TrunkGroup 0 = 0,0,0,16,16,7000,2;
TrunkGroup 0 = 0,1,1,16,16,7001,2;
TrunkGroup 0 = 0,2,2,16,16,7002,2;
TrunkGroup 0 = 0,3,3,16,16,7003,2;
[\\TrunkGroup]
[ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
CodersGroup0 0 = g7231;
CodersGroup0 1 = Transparent;
[ \\CodersGroup0 ]
[TelProfile]
FORMAT TelProfile_Index = TelProfile_ProfileName,
TelProfile_TelPreference, TelProfile_CodersGroupID,
TelProfile_IsFaxUsed, TelProfile_JitterBufMinDelay,
TelProfile_JitterBufOptFactor, TelProfile_IPDiffServ,
TelProfile_SigIPDiffServ, TelProfile_DtmfVolume,
TelProfile_InputGain, TelProfile_VoiceVolume,
TelProfile_EnableReversePolarity,
TelProfile_EnableCurrentDisconnect,
TelProfile_EnableDigitDelivery, TelProfile_EnableEC,
TelProfile_MWIAAnalog, TelProfile_MWIDisplay,
TelProfile_FlashHookPeriod, TelProfile_EnableEarlyMedia,
TelProfile_ProgressIndicator2IP;
TelProfile_1 = voice,$$,1,$$,,$$,,$$,,$$,,$$,,$$
TelProfile_2 = data,$$,2,$$,,$$,,$$,,$$,,$$,,$$
[\\TelProfile]
    
```

18.1.5.1.1 DSP Pattern Detector

For TDM tunneling applications, you can use the DSP pattern detector feature to initiate the echo canceller at call start. The device can be configured to support detection of a specific one-byte idle data pattern transmitted over digital E1/T1 timeslots. The device can be configured to detect up to four different one-byte data patterns. When the defined idle data pattern is detected, the channel resets its echo canceller.

The following parameters must be configured:

- EnableDSPIPMDetectors = 1
- EnablePatternDetector = 1
- PDThreshold - Pattern Detector Threshold, which defines the number of consecutive patterns to trigger the pattern detection event. For example: PDThreshold = 5
- PDPattern - Detection Pattern, which defines the patterns that can be detected by the Pattern Detector. For example: PDPattern = 84, 85, 212, 213 (for idle patterns: 54, 55, D4 and D5)

18.1.5.2 QSIG Tunneling

The device supports QSIG tunneling over SIP, according to IETF Internet-Draft draft-elwell-sipping-qsig-tunnel-03 ("Tunnelling of QSIG over SIP") and ECMA-355/ISO/IEC 22535. This is applicable to all ISDN variants. QSIG tunneling can be applied to all calls or to specific calls using IP Profiles.

QSIG tunneling sends all QSIG messages as raw data in corresponding SIP messages using a dedicated message body. This is used, for example, to enable two QSIG subscribers connected to the same or different QSIG PBX to communicate with each other over an IP network. Tunneling is supported in both directions (Tel-to-IP and IP-to-Tel).

The term tunneling means that messages are transferred 'as is' to the remote side without being converted (QSIG > SIP > QSIG). The advantage of tunneling over QSIG-to-SIP interworking is that by using interworking, QSIG functionality can only be partially achieved. When tunneling is used, all QSIG capabilities are supported and the tunneling medium (the SIP network) does not need to process these messages.

QSIG messages are transferred in SIP messages in a separate Multipurpose Internet Mail Extensions (MIME) body. Therefore, if a message contains more than one body (e.g., SDP and QSIG), multipart MIME must be used. The Content-Type of the QSIG tunneled message is 'application/QSIG'. The device also adds a Content-Disposition header in the following format:

```
Content-Disposition: signal; handling=required.
```

QSIG tunneling is done as follows:

- **Call setup (originating device):** The QSIG Setup request is encapsulated in the SIP INVITE message without being altered. After the SIP INVITE request is sent, the device does not encapsulate the subsequent QSIG message until a SIP 200 OK response is received. If the originating device receives a 4xx, 5xx, or 6xx response, it disconnects the QSIG call with a 'no route to destination' cause.
- **Call setup (terminating device):** After the terminating device receives a SIP INVITE request with a 'Content-Type: application/QSIG', it sends the encapsulated QSIG Setup message to the Tel side and sends a 200 OK response (no 1xx response is sent) to IP. The 200 OK response includes an encapsulated QSIG Call Proceeding message (without waiting for a Call Proceeding message from the Tel side). If tunneling is disabled and the incoming INVITE includes a QSIG body, a 415 response is sent.

- **Mid-call communication:** After the SIP connection is established, all QSIG messages are encapsulated in SIP INFO messages.
 - **Call tear-down:** The SIP connection is terminated once the QSIG call is complete. The Release Complete message is encapsulated in the SIP BYE message that terminates the session.
- **To enable QSIG tunneling:**
1. Set the EnableQSIGTunneling parameter to 1 on the originating and terminating devices.
 2. Configure the QSIGTunnelingMode parameter for defining the format of encapsulated QSIG message data in the SIP message MIME body (0 for ASCII presentation; 1 for binary encoding).
 3. Set the ISDNDuplicateQ931BuffMode parameter to 128 to duplicate all messages.
 4. Set the ISDNInCallsBehavior parameter to 4096.
 5. Set the ISDNRxOverlap parameter to 0 for tunneling of QSIG overlap-dialed digits (see below for description).

The configuration of the ISDNInCallsBehavior and ISDNRxOverlap parameters allows tunneling of QSIG overlap-dialed digits (Tel to IP). In this configuration, the device **delays** the sending of the QSIG Setup Ack message upon receipt of the QSIG Setup message. Instead, the device sends the Setup Ack message to QSIG only when it receives the SIP INFO message with Setup Ack encapsulated in its MIME body. The PBX sends QSIG Information messages (to complete the Called Party Number) only after it receives the Setup Ack. The device relays these Information messages encapsulated in SIP INFO messages to the remote party.

18.1.6 Advanced PSTN Configuration

This section describes various advanced PSTN configurations.

18.1.6.1 Release Reason Mapping

This section describes the available mapping mechanisms of SIP responses to Q.850 Release Causes and vice versa. The existing mapping of ISDN Release Causes to SIP Responses is described in 'Fixed Mapping of ISDN Release Reason to SIP Response' on page 241 and 'Fixed Mapping of SIP Response to ISDN Release Reason' on page 243. To override this hard-coded mapping and flexibly map SIP responses to ISDN Release Causes, use the *ini* file (CauseMapISDN2SIP and CauseMapSIP2ISDN, as described in 'ISDN and CAS Interworking Parameters' on page 686) or the Web interface (see 'Configuring Release Cause Mapping' on page 265).

It is also possible to map the less commonly used SIP responses to a single default ISDN Release Cause. Use the parameter DefaultCauseMapISDN2IP (described in 'ISDN and CAS Interworking Parameters' on page 686) to define a default ISDN Cause that is always used except when the following Release Causes are received: Normal Call Clearing (16), User Busy (17), No User Responding (18) or No Answer from User (19). This mechanism is only available for Tel-to-IP calls.

18.1.6.1.1 Reason Header

The device supports the Reason header according to RFC 3326. The Reason header conveys information describing the disconnection cause of a call:

- **Sending Reason header:** If a call is disconnected from the Tel side (ISDN), the Reason header is set to the received Q.850 cause in the appropriate message (BYE/CANCEL/final failure response) and sent to the SIP side. If the call is disconnected because of a SIP reason, the Reason header is set to the appropriate SIP response.

- **Receiving Reason header:** If a call is disconnected from the IP side and the SIP message includes the Reason header, it is sent to the Tel side according to the following logic:
 - If the Reason header includes a Q.850 cause, it is sent as is.
 - If the Reason header includes a SIP response:
 - ◆ If the message is a final response, the response status code is translated to Q.850 format and passed to ISDN.
 - ◆ If the message isn't a final response, it is translated to a Q.850 cause.
 - When the Reason header is received twice (i.e., SIP Reason and Q.850), the Q.850 takes precedence over the SIP reason and is sent to the Tel side.

18.1.6.1.2 Fixed Mapping of ISDN Release Reason to SIP Response

The following table describes the mapping of ISDN release reason to SIP response.

Table 18-2: Mapping of ISDN Release Reason to SIP Response

ISDN Release Reason	Description	SIP Response	Description
1	Unallocated number	404	Not found
2	No route to network	404	Not found
3	No route to destination	404	Not found
6	Channel unacceptable	406*	Not acceptable
7	Call awarded and being delivered in an established channel	500	Server internal error
16	Normal call clearing	-*	BYE
17	User busy	486	Busy here
18	No user responding	408	Request timeout
19	No answer from the user	480	Temporarily unavailable
21	Call rejected	403	Forbidden
22	Number changed w/o diagnostic	410	Gone
26	Non-selected user clearing	404	Not found
27	Destination out of order	502	Bad gateway
28	Address incomplete	484	Address incomplete
29	Facility rejected	501	Not implemented
30	Response to status enquiry	501*	Not implemented
31	Normal unspecified	480	Temporarily unavailable
34	No circuit available	503	Service unavailable
38	Network out of order	503	Service unavailable
41	Temporary failure	503	Service unavailable
42	Switching equipment congestion	503	Service unavailable
43	Access information discarded	502*	Bad gateway
44	Requested channel not available	503*	Service unavailable

ISDN Release Reason	Description	SIP Response	Description
47	Resource unavailable	503	Service unavailable
49	QoS unavailable	503*	Service unavailable
50	Facility not subscribed	503*	Service unavailable
55	Incoming calls barred within CUG	403	Forbidden
57	Bearer capability not authorized	403	Forbidden
58	Bearer capability not presently available	503	Service unavailable
63	Service/option not available	503*	Service unavailable
65	Bearer capability not implemented	501	Not implemented
66	Channel type not implemented	480*	Temporarily unavailable
69	Requested facility not implemented	503*	Service unavailable
70	Only restricted digital information bearer capability is available	503*	Service unavailable
79	Service or option not implemented	501	Not implemented
81	Invalid call reference value	502*	Bad gateway
82	Identified channel does not exist	502*	Bad gateway
83	Suspended call exists, but this call identity does not	503*	Service unavailable
84	Call identity in use	503*	Service unavailable
85	No call suspended	503*	Service unavailable
86	Call having the requested call identity has been cleared	408*	Request timeout
87	User not member of CUG	503	Service unavailable
88	Incompatible destination	503	Service unavailable
91	Invalid transit network selection	502*	Bad gateway
95	Invalid message	503	Service unavailable
96	Mandatory information element is missing	409*	Conflict
97	Message type non-existent or not implemented	480*	Temporarily not available
98	Message not compatible with call state or message type non-existent or not implemented	409*	Conflict
99	Information element non-existent or not implemented	480*	Not found
100	Invalid information elements contents	501*	Not implemented
101	Message not compatible with call state	503*	Service unavailable
102	Recovery of timer expiry	408	Request timeout

ISDN Release Reason	Description	SIP Response	Description
111	Protocol error	500	Server internal error
127	Interworking unspecified	500	Server internal error

* Messages and responses were created because the 'ISUP to SIP Mapping' draft doesn't specify their cause code mapping.

18.1.6.1.3 Fixed Mapping of SIP Response to ISDN Release Reason

The following table describes the mapping of SIP response to ISDN release reason.

Table 18-3: Mapping of SIP Response to ISDN Release Reason

SIP Response	Description	ISDN Release Reason	Description
400*	Bad request	31	Normal, unspecified
401	Unauthorized	21	Call rejected
402	Payment required	21	Call rejected
403	Forbidden	21	Call rejected
404	Not found	1	Unallocated number
405	Method not allowed	63	Service/option unavailable
406	Not acceptable	79	Service/option not implemented
407	Proxy authentication required	21	Call rejected
408	Request timeout	102	Recovery on timer expiry
409	Conflict	41	Temporary failure
410	Gone	22	Number changed w/o diagnostic
411	Length required	127	Interworking
413	Request entity too long	127	Interworking
414	Request URI too long	127	Interworking
415	Unsupported media type	79	Service/option not implemented
420	Bad extension	127	Interworking
480	Temporarily unavailable	18	No user responding
481*	Call leg/transaction doesn't exist	127	Interworking
482*	Loop detected	127	Interworking
483	Too many hops	127	Interworking
484	Address incomplete	28	Invalid number format
485	Ambiguous	1	Unallocated number
486	Busy here	17	User busy
488	Not acceptable here	31	Normal, unspecified

SIP Response	Description	ISDN Release Reason	Description
500	Server internal error	41	Temporary failure
501	Not implemented	38	Network out of order
502	Bad gateway	38	Network out of order
503	Service unavailable	41	Temporary failure
504	Server timeout	102	Recovery on timer expiry
505*	Version not supported	127	Interworking
600	Busy everywhere	17	User busy
603	Decline	21	Call rejected
604	Does not exist anywhere	1	Unallocated number
606*	Not acceptable	38	Network out of order

* Messages and responses were created because the 'ISUP to SIP Mapping' draft does not specify their cause code mapping.

18.1.6.2 ISDN Overlap Dialing

Overlap dialing is a dialing scheme used by several ISDN variants to send and/or receive called number digits one after the other (or several at a time). This is in contrast to en-bloc dialing in which a complete number is sent in one message. ISDN overlap dialing is applicable to PRI and BRI.

The device supports the following ISDN overlap dialing methods:

- Collects ISDN called party number digits and then sends the SIP INVITE to the IP side with the complete destination number (see 'Collecting ISDN Digits and Sending Complete Number in SIP' on page 244)
- Interworks ISDN overlap dialing with SIP, according to RFC 3578 (see 'Interworking ISDN Overlap Dialing with SIP According to RFC 3578' on page 245)

18.1.6.2.1 Collecting ISDN Digits and Sending Complete Number in SIP

The device can support an overlap dialing mode whereby the device collects the called party number digits from ISDN Q.931 Information messages or DTMF signals, and then sends a SIP INVITE message to the IP side containing the complete destination number.

ISDN overlap dialing for incoming ISDN calls can be configured for the entire device or per E1/T1 trunk. This is configured using the global, ISDNRxOverlap parameter or the ISDNRxOverlap_x parameter (where x depicts the trunk number), respectively.

By default (see the ISDNINCallsBehavior parameter), the device plays a dial tone to the ISDN user side when it receives an empty called number from the ISDN. In this scenario, the device includes the Progress Indicator in the SetupAck ISDN message that it sends to the ISDN side.

The device can also mute in-band DTMF detection until it receives the complete destination number from the ISDN. This is configured using the MuteDTMFInOverlap parameter. The Information digits can be sent in-band in the voice stream, or out-of-band using Q.931 Information messages. If Q.931 Information messages are used, the DTMF in-band detector must be disabled. Note that when at least one digit is received in the ISDN Setup message, the device stops playing a dial tone.

The device stops collecting digits (from the ISDN) upon the following scenarios:

- The device receives a Sending Complete IE in the ISDN Setup or Information messages, indicating no more digits.
- The timeout between received digits expires (configured by the TimeBetweenDigits parameter).
- The maximum number of received digits has been reached (configured by the MaxDigits parameter).
- A match is found with the defined digit map (configured by the DigitMapping parameter).

Relevant parameters (described in 'PSTN Parameters' on page 670):

- ISDNRxOverlap_x = 1 (can be configured per trunk)
- TimeBetweenDigits
- MaxDigits
- MuteDTMFInOverlap
- DigitMapping

For configuring ISDN overlap dialing using the Web interface, see 'Configuring Trunk Settings' on page 232.

18.1.6.2.2 Interworking ISDN Overlap Dialing with SIP According to RFC 3578

The device supports the interworking of ISDN overlap dialing to SIP and vice versa, according to RFC 3578.

- **Interworking ISDN overlap dialing to SIP (Tel to IP):** The device sends collected digits each time it receives them (initially from the ISDN Setup message and then from subsequent Q.931 Information messages) to the IP side, using subsequent SIP INVITE messages. You can also define the minimum number of overlap digits to collect before sending the first SIP message (INVITE) for routing the call, using the MinOverlapDigitsForRouting parameter.
- **Interworking SIP to ISDN overlap dialing (IP to Tel):** For each received SIP INVITE pertaining to the same dialog session, the device sends an ISDN Setup message (and subsequent Q.931 Information messages) with the collected digits to the Tel side. For all subsequent INVITEs received, the device sends a SIP 484 "Address Incomplete" response to the IP in order to maintain the current dialog session and to receive additional digits from subsequent INVITEs.

Relevant parameters (described in 'PSTN Parameters' on page 670):

- ISDNRxOverlap = 2
- ISDNTxOverlap
- ISDNOutCallsBehavior = 2
- MinOverlapDigitsForRouting
- TimeBetweenDigits
- MaxDigits
- DigitMapping
- MuteDTMFInOverlap

For configuring ISDN overlap dialing using the Web interface, see 'Configuring Trunk Settings' on page 232.

18.1.6.3 ISDN Non-Facility Associated Signaling (NFAS)

In regular T1 ISDN trunks, a single 64 kbps channel carries signaling for the other 23 B-channels of that particular T1 trunk. This channel is called the D-channel and usually resides on timeslot # 24. The ISDN Non-Facility Associated Signaling (NFAS) feature enables the use of a single D-channel to control multiple PRI interfaces.

With NFAS it is possible to define a group of T1 trunks, called an NFAS group, in which a single D-channel carries ISDN signaling messages for the entire group. The NFAS group's B-channels are used to carry traffic such as voice or data. The NFAS mechanism also enables definition of a backup D-channel on a different T1 trunk, to be used if the primary D-channel fails.

The device supports up to 12 NFAS groups. Each group can comprise up to 10 T1 trunks and each group must contain different T1 trunks. Each T1 trunk is called an 'NFAS member'. The T1 trunk whose D-channel is used for signaling is called the 'Primary NFAS Trunk'. The T1 trunk whose D-channel is used for backup signaling is called the 'Backup NFAS Trunk'. The primary and backup trunks each carry 23 B-channels while all other NFAS trunks each carry 24 B-channels.

The NFAS group is identified by an NFAS GroupID number (possible values are 1 to 12). To assign a number of T1 trunks to the same NFAS group, use the ini file parameter `NFASGroupNumber_x = groupID` (where x is the physical trunk ID (0 to the maximum number of trunks) or the Web interface (see [Configuring Trunk Settings](#) on page 232).

The parameter `DchConfig_x = Trunk_type` defines the type of NFAS trunk. `Trunk_type` is set to 0 for the primary trunk, to 1 for the backup trunk, and to 2 for an ordinary NFAS trunk. 'x' depicts the physical trunk ID (0 to the maximum number of trunks). You can also use the Web interface (see [Configuring Trunk Settings](#) on page 232).

For example, to assign the first four T1 trunks to NFAS group #1, in which trunk #0 is the primary trunk and trunk #1 is the backup trunk, use the following configuration:

```
NFASGroupNumber_0 = 1
NFASGroupNumber_1 = 1
NFASGroupNumber_2 = 1
NFASGroupNumber_3 = 1
DchConfig_0 = 0           ;Primary T1 trunk
DchConfig_1 = 1           ;Backup T1 trunk
DchConfig_2 = 2           ;24 B-channel NFAS trunk
DchConfig_3 = 2           ;24 B-channel NFAS trunk
```

The NFAS parameters are described in 'PSTN Parameters' on page 670.

18.1.6.3.1 NFAS Interface ID

Several ISDN switches require an additional configuration parameter per T1 trunk that is called 'Interface Identifier'. In NFAS T1 trunks, the Interface Identifier is sent explicitly in Q.931 Setup / Channel Identification IE for all NFAS trunks, except for the B-channels of the Primary trunk (see note below).

The Interface ID can be defined per member (T1 trunk) of the NFAS group, and must be coordinated with the configuration of the Switch. The default value of the Interface ID is identical to the number of the physical T1 trunk (0 for the first trunk, 1 for the second T1 trunk, and so on, up to the maximum number of trunks).

To define an explicit Interface ID for a T1 trunk (that is different from the default), use the following parameters:

- `ISDNIBehavior_x = 512` (x = 0 to the maximum number of trunks identifying the device's physical trunk)
- `ISDNNFASInterfaceID_x = ID` (x = 0 to 255)

**Notes:**

- Usually the Interface Identifier is included in the Q.931 Setup/Channel Identification IE only on T1 trunks that doesn't contain the D-channel. Calls initiated on B-channels of the Primary T1 trunk, by default, don't contain the Interface Identifier. Setting the parameter ISDNIBehavior_x to 2048' forces the inclusion of the Channel Identifier parameter also for the Primary trunk.
- The parameter ISDNNFASInterfaceID_x = ID can define the 'Interface ID' for any Primary T1 trunk, even if the T1 trunk is not a part of an NFAS group. However, to include the Interface Identifier in Q.931 Setup/Channel Identification IE configure ISDNIBehavior_x = 2048 in the *ini* file.

18.1.6.3.2 Working with DMS-100 Switches

The DMS-100 switch requires the following NFAS Interface ID definitions:

- InterfaceID #0 for the Primary trunk
- InterfaceID #1 for the Backup trunk
- InterfaceID #2 for a 24 B-channel T1 trunk
- InterfaceID #3 for a 24 B-channel T1 trunk, and so on for subsequent T1 trunks

For example, if four T1 trunks on a device are configured as a single NFAS group with Primary and Backup T1 trunks that is used with a DMS-100 switch, the following parameters should be used:

```
NFASGroupNumber_0 = 1
NFASGroupNumber_1 = 1
NFASGroupNumber_2 = 1
NFASGroupNumber_3 = 1
DchConfig_0 = 0 ;Primary T1 trunk
DchConfig_1 = 1 ;Backup T1 trunk
DchConfig_2 = 2 ;B-Channel NFAS trunk
DchConfig_3 = 2 ;B-channel NFAS trunk
```

If there is no NFAS Backup trunk, the following configuration should be used:

```
ISDNNFASInterfaceID_0 = 0
ISDNNFASInterfaceID_1 = 2
ISDNNFASInterfaceID_2 = 3
ISDNNFASInterfaceID_3 = 4
ISDNIBehavior = 512 ;This parameter should be added because of
;ISDNNFASInterfaceID configuration above
NFASGroupNumber_0 = 1
NFASGroupNumber_1 = 1
NFASGroupNumber_2 = 1
NFASGroupNumber_3 = 1
DchConfig_0 = 0 ;Primary T1 trunk
DchConfig_1 = 2 ;B-Channel NFAS trunk
DchConfig_2 = 2 ;B-Channel NFAS trunk
DchConfig_3 = 2 ;B-channel NFAS trunk
```

18.1.6.3.3 Creating an NFAS-Related Trunk Configuration

The procedures for creating and deleting an NFAS group must be performed in the correct order, as described below.

➤ **To create an NFAS Group:**

1. If there's a backup ('secondary') trunk for this group, it must be configured first.
2. Configure the primary trunk before configuring any NFAS ('slave') trunk.
3. Configure NFAS ('slave') trunks.

➤ **To stop / delete an NFAS Group:**

1. Stop or delete (by setting ProtocolType to 0, i.e., 'None') all NFAS ('slave') trunks.
2. Stop or delete (by setting ProtocolType to 0, i.e., 'None') the backup trunk if a backup trunk exists.
3. Stop or delete (by setting ProtocolType to 0, i.e., 'None') the primary trunk.



Notes:

- All trunks in the group must be configured with the same values for trunk parameters TerminationSide, ProtocolType, FramingMethod, and LineCode.
- After stopping or deleting the backup trunk, delete the group and then reconfigure it.

18.1.6.4 Redirect Number and Calling Name (Display)

The following tables define the device's redirect number and calling name (Display) support for various ISDN variants according to NT (Network Termination) / TE (Termination Equipment) interface direction:

Table 18-4: Calling Name (Display)

NT/TE Interface	DMS-100	NI-2	4/5ESS	Euro ISDN	QSIG
NT-to-TE	Yes	Yes	No	Yes	Yes
TE-to-NT	Yes	Yes	No	No	Yes

Table 18-5: Redirect Number

NT/TE Interface	DMS-100	NI-2	4/5ESS	Euro ISDN	QSIG
NT-to-TE	Yes	Yes	Yes	Yes	Yes
TE-to-NT	Yes	Yes	Yes	Yes*	Yes

* When using ETSI DivertingLegInformation2 in a Facility IE (not Redirecting Number IE).

18.2 Trunk Group

This section describes the configuration of the device's channels, which entails assigning them numbers and Trunk Group IDs.

18.2.1 Configuring Trunk Group Table

The Trunk Group Table page allows you to define up to 120 Trunk Groups. A Trunk Group is a logical group of physical trunks and channels, and is assigned an ID. The Trunk Group can include multiple trunks and ranges of channels.

To enable and activate the channels of the device, Trunk Groups need to be defined and with telephone numbers. Channels that are not defined in this table are disabled. The Trunk Groups are later used for routing IP-to-Tel and Tel-to-IP calls.



Note: You can also configure Trunk Groups using the *ini* file table parameter `TrunkGroup_x` to (see 'Number Manipulation Parameters' on page 732).

➤ **To configure the Trunk Group Table:**

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

Add Phone Context As Prefix		Disable					
Trunk Group Index		1-12					
Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 PRI	1	1	1-30	6000	1	1
2	Module 1 PRI	2	2	1-30	7000	2	1
3	Module 2 FXS			1-4	101	3	2
4							

2. Configure the Trunk Group according to the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to the flash memory, see 'Saving Configuration' on page 470.
5. To register the Trunk Groups, click the **Register** button. To unregister the Trunk Groups, click **Unregister**. The registration method for each Trunk Group is according to the setting of the 'Registration Mode' parameter in the Trunk Group Settings page.

Table 18-6: Trunk Group Table Parameters

Parameter	Description
Module [TrunkGroup_Module]	The module (i.e., FXS, FXO, PRI, or BRI) for which you want to define the Trunk Group.

Parameter	Description
From Trunk [TrunkGroup_FirstTrunkId]	Starting physical Trunk number in the Trunk Group. The number of listed Trunks depends on the device's hardware configuration. Note: This parameter is applicable only to PRI and BRI modules.
To Trunk [TrunkGroup_LastTrunkId]	Ending physical Trunk number in the Trunk Group. The number of listed Trunks depends on the device's hardware configuration. Note: This parameter is applicable only to PRI and BRI modules.
Channels [TrunkGroup_FirstBChannel], [TrunkGroup_LastBChannel]	The device's channels/ports (analog module) or Trunk B-channels (digital module). To enable channels, enter the channel numbers. You can enter a range of channels by using the format [n-m], where <i>n</i> represents the lower channel number and <i>m</i> the higher channel number. For example, [1-4] specifies channels 1 through 4. Notes: <ul style="list-style-type: none"> The number of defined channels must not exceed the maximum number of the Trunk's B-channels. To represent all the Trunk's B-channels, enter a single asterisk (*).
Phone Number [TrunkGroup_FirstPhoneNumber]	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 numbers are also used for channel allocation for IP-to-Tel calls if the Trunk Group's 'Channel Select Mode' is set to 'By Dest Phone Number'. Notes: <ul style="list-style-type: none"> 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'). This field is optional for BRI/PRI interfaces. The logical numbers defined in this field are used when an incoming PSTN/PBX call doesn't contain the calling number or called number (the latter being determined by the ReplaceEmptyDstWithPortNumber parameter). These numbers are used to replace them.
Trunk Group ID [TrunkGroup_TrunkGroupNum]	The Trunk Group ID (0-119) assigned to the corresponding channels. The same Trunk Group ID can be assigned to more than one group of channels. The Trunk Group ID is used to define a group of common channel behavior that are used for routing IP-to-Tel calls. If an IP-to-Tel call is assigned to a Trunk Group, the IP call is routed to the channel(s) pertaining to that Trunk Group ID. Notes: <ul style="list-style-type: none"> Once you have defined a Trunk Group, you must configure the parameter PSTNPrefix (Inbound IP Routing Table) to assign incoming IP calls to the appropriate Trunk Group. If you do not configure this, calls cannot be established. You can define the method for which calls are assigned to channels within Trunk Groups, using the parameter TrunkGroupSettings.
Tel Profile ID [TrunkGroup_ProfileId]	The Tel Profile ID assigned to the channels pertaining to the Trunk Group. Note: For configuring Tel Profiles, refer to the parameter TelProfile.

18.2.2 Configuring Trunk Group Settings

The Trunk Group Settings page allows you to configure the settings of up to 120 Trunk Groups. These Trunk Groups are configured in the Trunk Group Table page (see [Configuring Trunk Group Table](#) on page 249).

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



Note: You can also configure the Trunk Group Settings table using the *ini* file table parameter TrunkGroupSettings (see 'Number Manipulation Parameters' on page 732).

➤ **To configure the Trunk Group Settings table:**

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

Index					
					1-12
Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	Cyclic Ascending	Per Gateway	1		
2					
3					
4					

2. From the 'Index' drop-down list, select the range of entries that you want to edit.
3. Configure the Trunk Group according to the table below.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 470.

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 193).

```
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: 9907977062512000232825@10.33.37.78
CSeq: 3 REGISTER
Contact: <sip:101@10.33.37.78>;expires=3600
Expires: 3600
User-Agent: Sip-Gateway/v.6.00A.008.002
Content-Length: 0
```

Table 18-7: Trunk Group Settings Parameters

Parameter	Description
Trunk Group ID [TrunkGroupSettings_TrunkGroupId]	The Trunk Group ID that you want to configure.
Channel Select Mode [TrunkGroupSettings_ChannelSelectMode]	<p>The method for which IP-to-Tel calls are assigned to channels pertaining to a Trunk Group. For a detailed description of this parameter, refer to the global parameter ChannelSelectMode.</p> <ul style="list-style-type: none"> ▪ [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 ▪ [7] Trunk Cyclic Ascending (applicable only to digital interfaces) ▪ [8] Trunk & Channel Cyclic Ascending (applicable only to digital interfaces) ▪ [9] Ring to Hunt Group (applicable only to FXS interfaces) ▪ [10] Select Trunk by Supplementary Services Table (applicable only to BRI interfaces) ▪ [11] Dest Number + Ascending <p>Note: For a detailed description of these options, refer to the "global" ChannelSelectMode parameter.</p>
Registration Mode [TrunkGroupSettings_RegistrationMode]	<p>Registration method for the Trunk Group:</p> <ul style="list-style-type: none"> ▪ [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 Trunk 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 Trunk Group. For example, if the device is configured globally to register all its endpoints (using the parameter ChannelSelectMode), you can exclude some endpoints from being registered by assigning them to a Trunk Group and configuring the Trunk Group registration mode to 'Don't Register'. ▪ [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 223). <p>Notes:</p> <ul style="list-style-type: none"> ▪ To enable Trunk 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

Parameter	Description
	<p>the global registration parameter ChannelSelectMode.</p> <ul style="list-style-type: none"> ▪ If the device is configured globally (ChannelSelectMode) to register Per Endpoint, and channels group comprising four channels is configured to register Per Gateway, the device registers all channels except the first four channels. The channels Group of these four channels sends a single registration request.
<p>Serving IP Group ID [TrunkGroupSettings_Servi ngIPGroup]</p>	<p>The Serving IP Group ID to where INVITE messages initiated by this Trunk 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 198) 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 193). If no Serving IP Group ID is selected, the INVITE messages are sent to the default Proxy or according to the Outbound IP Routing Table (see 'Configuring Outbound IP Routing Table' on page 269).</p> <p>Note: If the parameter PreferRouteTable is set to 1 (see 'Configuring Proxy and Registration Parameters' on page 226), the routing rules in the Outbound IP Routing Table prevail over the selected Serving IP Group ID.</p>
<p>Gateway Name [TrunkGroupSettings_Gate wayName]</p>	<p>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.</p>
<p>Contact User [TrunkGroupSettings_Conta ctUser]</p>	<p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.

18.3 Manipulation

This section describes the configuration of number / name manipulation rules and various SIP to non-SIP mapping.

18.3.1 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 529.

➤ **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 18-4: General Settings Page

Set TEL-to-IP Redirect Reason	Not Configured	▼
Set IP-to-TEL Redirect Reason	Not Configured	▼
Set Redirect number Screening Indicator to TEL	Not Configured	▼

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

18.3.2 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 source telephone numbers so that the calls can be routed correctly. The number manipulation tables include the following:

■ **Tel-to-IP calls:**

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

■ **IP-to-Tel calls:**

- Destination Phone Number Manipulation Table for IP-to-Tel Calls table (NumberMapIP2Tel *ini* file parameter) - up to 100 entries
- Source Phone Number Manipulation Table for IP-to-Tel Calls table (SourceNumberMapIP2Tel *ini* file parameter) - up to 120 entries

The manipulation rules can be applied to incoming calls that match one or any combination of the following characteristics:

- Source Trunk Group
- Source IP Group
- Destination (called) number prefix or suffix
- Source (calling) number prefix or suffix
- Source IP address

The device manipulates the number in the following order:

1. Strips digits from the left of the number.
2. Strips digits from the right of the number.
3. Retains the defined number of digits.
4. Adds the defined prefix.
5. Adds the defined suffix.

The device searches a matching manipulation rule starting from the first entry (i.e., top of the table). In other words, a rule at the top of the table takes precedence over a rule defined lower down in the table. Therefore, define more specific rules above more generic rules. For example, if you enter 551 in Index 1 and 55 in Index 2, the device applies rule 1 to numbers that start with 551 and applies rule 2 to numbers that start with 550, 552, 553, and so on until 559. However, if you enter 55 in Index 1 and 551 in Index 2, the device applies rule 1 to all numbers that start with 55, including numbers that start with 551.

You can perform a second "round" (additional) of destination (NumberMapIP2Tel parameter) and source (SourceNumberMapIP2Tel parameter) number manipulations for IP-to-Tel calls on an already manipulated number. The initial and additional number manipulation rules are both configured in these tables. The additional manipulation is performed on the initially manipulated number. Therefore, for complex number manipulation schemes, you only need to configure relatively few manipulation rules in these tables (that would otherwise require many rules). This feature is enabled using the following parameters:

- PerformAdditionalIP2TELSrcManipulation for source number manipulation
- PerformAdditionalIP2TELDestinationManipulation for destination number manipulation

Telephone number manipulation can be useful, for example, for doing the following:

- Stripping or adding dialing plan digits from or to the number, respectively. For example, a user may need to first dial 9 before dialing the phone number to indicate an external line. This number 9 can then be removed by number manipulation before the call is setup.
- Allowing or blocking Caller ID information according to destination or source prefixes. For more information on Caller ID, see [Configuring Caller Display Information](#) on page 318.
- For digital modules only: Assigning Numbering Plan Indicator (NPI) and Type of Numbering (TON) to IP-to-Tel calls. The device can use a single global setting for NPI/TON classification or it can use the setting in the manipulation tables on a call-by-call basis.



Notes:

- Number manipulation can occur before or after a routing decision is made. For example, you can route a call to a specific Trunk Group according to its original number, and then you can remove or add a prefix to that number before it is routed. To determine when number manipulation is performed, configure the 'IP to Tel Routing Mode' parameter (RouteModeIP2Tel) described in 'Configuring Inbound IP Routing Table' on page 277, and 'Tel to IP Routing Mode' parameter (RouteModeTel2IP) described in 'Configuring Outbound IP Routing Table' on page 269.
- For configuring number manipulation using *ini* file table parameters NumberMapIP2Tel, NumberMapTel2IP, SourceNumberMapIP2Tel, and SourceNumberMapTel2IP, see 'Number Manipulation Parameters' on page 732.

➤ **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 18-5: 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 previous figure 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 **Submit** to apply your changes.
 4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

Table 18-8: Number Manipulation Parameters Description

Parameter	Description
Source Trunk Group	The source Trunk Group ID for Tel-to-IP calls. To denote all Trunk Groups, leave this field empty. Notes: <ul style="list-style-type: none"> ▪ 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

Parameter	Description
	<p>'Inbound IP Routing Table'. If not used (i.e., any IP Group), simply leave the field empty.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 and/or suffix. For example, [100-199](100,101,105) depicts a number that starts with 100 to 199 and ends with 100, 101 or 105. For a description of notations that you can use to represent single and multiple numbers (ranges), see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 767 .
Web/EMS: Source Prefix	Source (calling) telephone number prefix and/or suffix. For example, [100-199](100,101,105) depicts a number that starts with 100 to 199 and ends with 100, 101 or 105. For a description of notations that you can use to represent single and multiple numbers (ranges), see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 767 .
Web/EMS: Source IP Address	Source IP address of the caller (obtained from the Contact header in the INVITE message). <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.
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.

Parameter	Description
Web: NPI EMS: Number Plan	The Numbering Plan Indicator (NPI) assigned to this entry. <ul style="list-style-type: none"> ▪ [0] Unknown (default) ▪ [9] Private ▪ [1] E.164 Public ▪ [-1] Not Configured = value received from PSTN/IP is used Notes: <ul style="list-style-type: none"> ▪ This parameter is applicable only to Number Manipulation tables for IP-to-Tel calls. ▪ For more information on available NPI/TON values, see Numbering Plans and Type of Number on page 264
Web: TON EMS: Number Type	The Type of Number (TON) assigned to this entry. <ul style="list-style-type: none"> ▪ If you selected 'Unknown' for the NPI, you can select Unknown [0]. ▪ If you selected 'Private' for the NPI, you can select Unknown [0], Level 2 Regional [1], Level 1 Regional [2], PISN Specific [3] or Level 0 Regional (Local) [4]. ▪ If you selected 'E.164 Public' for the NPI, you can select Unknown [0], International [1], National [2], Network Specific [3], Subscriber [4] or Abbreviated [6]. Notes: <ul style="list-style-type: none"> ▪ This parameter is applicable only to Number Manipulation tables for IP-to-Tel calls. ▪ The default is 'Unknown'.
Web: Presentation EMS: Is Presentation Restricted	Determines whether Caller ID is permitted: <ul style="list-style-type: none"> ▪ Not Configured = Privacy is determined according to the Caller ID table (see Configuring Caller Display Information on page 318). ▪ [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: <ul style="list-style-type: none"> ▪ This field is applicable only to Number Manipulation tables for 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.

18.3.3 Configuring Redirect Number IP to Tel

The Redirect Number IP > Tel page allows you to configure IP-to-Tel redirect number manipulation rules. This feature allows you to manipulate the value of the received SIP Diversion, Resource-Priority, or History-Info headers, which is then added to the Redirecting Number Information Element (IE) in the ISDN Setup message that is sent to the Tel side.

**Notes:**

- You can also configure the Redirect Number IP to Tel table using the *ini* file parameter RedirectNumberMapIp2Tel (see 'Number Manipulation Parameters' on page 732).
- 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 done in the following order: Stripped Digits From Left, Stripped Digits From Right, Number of Digits to Leave, Prefix to Add, and then Suffix to Add.
- The Destination Number and Redirect Prefix parameters are used before any manipulation has been done on them.

➤ **To configure Redirect Number IP-to-Tel manipulation rules:**

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

Figure 18-6: Redirect Number IP to Tel Page

Index	Destination Prefix	Redirect Prefix	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add	Suffix to Add	
1	*	*	0	0			
			Number of Digits to Leave	Presentation	Source IP Address	TON	NPI
			255	Not Configured	*	Not Configured	Not Configured

2. Configure the rules according to the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

Table 18-9: Redirect Number IP to Tel Parameters Description

Parameter	Description
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.

Parameter	Description
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.
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	<p>Determines whether Caller ID is permitted:</p> <ul style="list-style-type: none"> Not Configured = Privacy is determined according to the Caller ID table (see Configuring Caller Display Information on page 318). [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. <p>Notes:</p> <ul style="list-style-type: none"> 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.
Web/EMS: Source IP Address	<p>Source IP address of the caller (obtained from the Contact header in the INVITE message).</p> <p>Note: The source IP address can include the following wildcards:</p> <ul style="list-style-type: none"> "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: TON EMS: Number Type	<p>The Type of Number (TON) assigned to this entry. The default is 'Unknown' [0].</p> <ul style="list-style-type: none"> If you select 'Unknown' for the NPI, you can select Unknown [0]. If you select 'Private' for the NPI, you can select Unknown [0], International [1], National [2], Network Specific [3] or Subscriber [4]. If you select 'E.164 Public' for the NPI, you can select Unknown [0], International [1], National [2], Network Specific [3], Subscriber [4] or Abbreviated [6].
Web: NPI EMS: Number Plan	<p>The Numbering Plan Indicator (NPI) assigned to this entry.</p> <ul style="list-style-type: none"> [0] Unknown (default) [9] Private [1] E.164 Public [-1] Not Configured = value received from PSTN/IP is used <p>Note: For more information on available NPI/TON values, see 'Numbering Plans and Type of Number' on page 264.</p>

18.3.4 Configuring Redirect Number Tel to IP

The Redirect Number Tel > IP page allows 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 Parameters' on page 732).
- 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 18-7: Redirect Number Tel to IP Page

Index	Source Trunk Group	Source IP Group	Destination Prefix	Redirect Prefix	Stripped Digits From Left	Stripped Digits From Right	Prefix to Add
1	-1	-1	*	555	3	0	9
				Suffix to Add	Number of Digits to Leave		Presentation
					255		Not Configured

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 **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

Table 18-10: Redirect Number Tel to IP Parameters Description

Parameter	Description
Source Trunk Group	The Trunk Group from where the Tel call is received. To denote any Trunk Group, leave this field empty. Notes: <ul style="list-style-type: none"> ▪ The value -1 indicates that this field is ignored in the rule. ▪ 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, the IP Group of an incoming INVITE is determined/classified using the 'Inbound IP Routing Table'. If not used (i.e., any IP Group), simply leave

Parameter	Description
	the field empty. Notes: <ul style="list-style-type: none"> 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.
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: <ul style="list-style-type: none"> Not Configured = Privacy is determined according to the Caller ID table (see Configuring Caller Display Information on page 318). [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.

18.3.5 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 ISDN/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 18-8: Phone Context Table Page

Add Phone Context As Prefix		Enable
Phone Context Index		1-10
NPI	TON	Phone Context
1	Unknown	unknown.com
2	Private	host.com
3	E.164 Public	na.e164.host.com
4		

2. Configure the Phone Context table according to the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.



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 Parameters' on page 732).

Table 18-11: 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 ISDN SETUP message (digital interfaces) with Called and Calling numbers. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
NPI	Select the Number Plan assigned to this entry. <ul style="list-style-type: none"> ▪ [0] Unknown (default) ▪ [1] E.164 Public ▪ [9] Private For a detailed list of the available NPI/TON values, see Numbering Plans and Type of Number on page 264.
TON	Select the Type of Number assigned to this entry. <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ✓ [0] Unknown ✓ [1] Level 2 Regional

Parameter	Description
	<ul style="list-style-type: none"> ✓ [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: <ul style="list-style-type: none"> ✓ [0] Unknown ✓ [1] International ✓ [2] National ✓ [3] Network Specific ✓ [4] Subscriber ✓ [6] Abbreviated
Phone Context	The Phone-Context SIP URI parameter.

18.3.6 Numbering Plans and Type of Number

The IP-to-Tel destination or source number manipulation tables allow you to classify numbers by their Numbering Plan Indication (NPI) and Type of Number (TON). The device supports all NPI/TON classifications used in the standard. The list of ETSI ISDN NPI/TON values is shown in the following table:

Table 18-12: NPI/TON Values for ETSI ISDN Variant

NPI	TON	Description
Unknown [0]	Unknown [0]	A valid classification, but one that has no information about the numbering plan.
E.164 Public [1]	Unknown [0]	A public number in E.164 format, but no information on what kind of E.164 number.
	International [1]	A public number in complete international E.164 format, e.g., 16135551234.
	National [2]	A public number in complete national E.164 format, e.g., 6135551234.
	Network Specific [3]	The type of number "network specific number" is used to indicate administration / service number specific to the serving network, e.g., used to access an operator.
	Subscriber [4]	A public number in complete E.164 format representing a local subscriber, e.g., 5551234.
	Abbreviated [6]	The support of this code is network dependent. The number provided in this information element presents a shorthand representation of the complete number in the specified numbering plan as supported by the network.
Private [9]	Unknown [0]	A private number, but with no further information about the numbering plan.
	Level 2 Regional [1]	
	Level 1 Regional [2]	A private number with a location, e.g., 3932200.
	PISN Specific [3]	
	Level 0 Regional (local) [4]	A private local extension number, e.g., 2200.

For NI-2 and DMS-100 ISDN variants, the valid combinations of TON and NPI for calling and called numbers include (Plan/Type):

- 0/0 - Unknown/Unknown
- 1/1 - International number in ISDN/Telephony numbering plan
- 1/2 - National number in ISDN/Telephony numbering plan
- 1/4 - Subscriber (local) number in ISDN/Telephony numbering plan
- 9/4 - Subscriber (local) number in Private numbering plan

18.3.7 Configuring Release Cause Mapping

The Release Cause Mapping page consists of two groups that allow the device to map up to 12 different SIP Response Codes to ITU-T Q.850 Release Cause Codes and vice versa, thereby overriding the hard-coded mapping mechanism (described in 'Release Reason Mapping' on page 240).



Note: You can also configure SIP Responses-Q.850 Release Causes mapping using the *ini* file table parameters CauseMapISDN2SIP and CauseMapSIP2ISDN (see 'ISDN and CAS Interworking-Related Parameters' on page 686).

➤ **To configure Release Cause Mapping:**

1. Open the Release Cause Mapping page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** submenu > **Release Cause Mapping**).

Figure 18-9: Release Cause Mapping Page

Release Cause Mapping from ISDN to SIP			
	Q.850 Cause		SIP Response
1	<input type="text"/>		<input type="text"/>
2	<input type="text"/>		<input type="text"/>
3	<input type="text"/>		<input type="text"/>
4	<input type="text"/>		<input type="text"/>
5	<input type="text"/>		<input type="text"/>
6	<input type="text"/>		<input type="text"/>
7	<input type="text"/>		<input type="text"/>
8	<input type="text"/>		<input type="text"/>
9	<input type="text"/>		<input type="text"/>
10	<input type="text"/>		<input type="text"/>
11	<input type="text"/>		<input type="text"/>
12	<input type="text"/>		<input type="text"/>

Release Cause Mapping from SIP to ISDN			
	SIP Response		Q.850 Cause
1	<input type="text"/>		<input type="text"/>
2	<input type="text"/>		<input type="text"/>
3	<input type="text"/>		<input type="text"/>

2. In the 'Release Cause Mapping from ISDN to SIP' group, map different Q.850 Release Causes to SIP Responses.
3. In the 'Release Cause Mapping from SIP to ISDN' group, map different SIP Responses to Q.850 Release Causes.
4. Click **Submit** to apply your changes.

18.3.8 SIP Calling Name Manipulations

You can configure manipulation rules for manipulating the calling name (i.e., caller ID) in the SIP message. This can include modifying or removing the calling name. SIP calling name manipulation is applicable to Tel-to-IP and IP-to-Tel calls.

For example, assume that an incoming SIP INVITE message includes the following header:

```
P-Asserted-Identity: "company:john" sip:66666@78.97.79.104
```

Using the IP-to-Tel calling name manipulation, the text, "company" can be changed to "worker" in the outgoing INVITE, as shown below:

```
P-Asserted-Identity: "worker:john" sip:9966666@10.13.83.10
```

To manipulate the calling name received in the SIP message, use the following parameters:

- For IP-to-Tel calls, use the CallingNameMapIp2Tel ini file parameter
- For Tel-to-IP calls, use the CallingNameMapTel2Ip ini file parameter

18.3.9 SIP Message Manipulation

You can manipulate SIP messages using the Message Manipulations table. This can be configured using the MessageManipulations ini file parameter. This manipulation includes insertion, removal, and/or modification of SIP headers. Multiple manipulation rules can be configured for the same SIP message.

Once you have defined SIP message manipulation rules (*Manipulation Set ID*), you can assign them to inbound and outbound SIP messages:

- For manipulation on all inbound SIP INVITE messages, the Manipulation Set ID is selected (and enabled) using the "global" parameter, GWInboundManipulationSet.
- For manipulation on outbound SIP INVITE messages, the Manipulation Set ID is selected (and enabled) using the following logic:
 - a. According to the settings of the Outbound Message Manipulation Set parameter of the destination IP Group table. In other words, manipulation can be done per destination IP Group. If this parameter is not configured, see b below.
 - b. According to the settings of the "global" parameter, GWOutboundManipulationSet. If this parameter is also not configured, no manipulation is done.

**Notes:**

- Each message can be manipulated twice - once for the source leg manipulation rules and once in the destination leg (source and destination IP Groups).
- Unknown SIP parts can only be added or removed.
- SIP manipulations do not allow you to remove or add mandatory SIP headers. They can only be modified and only on requests that initiate new dialogs. Mandatory SIP headers include To, From, Via, CSeq, Call-Id, and Max-Forwards.
- Manipulation of SDP body is currently not supported.
- For the IP-to-IP application, the outgoing message is re-created and thus, SIP headers not relevant to the outgoing SIP session (e.g., Referred-By) are not included in the outgoing message. Therefore, if required, manipulations on such headers should be handled in inbound manipulation.

18.3.10 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 254):

$x[n,l]y...$

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.

- The first seven digits from the left are removed from the original number, by entering "7" in the 'Stripped Digits From Left' field.

Figure 18-10: 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.

18.4 Routing

This section describes the configuration of call routing rules.

18.4.1 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 529.

- **To configure general routing parameters:**

- Open the Routing General Parameters page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** submenu > **General Parameters**).

General Parameters	
Add Hunt Group ID as Prefix	No
Add Trunk ID as Prefix	No
Replace Empty Destination with B-channel Phone Number	No
Add NPI and TON to Called Number	No
Add NPI and TON to Calling Number	No
IP to Tel Remove Routing Table Prefix	No
Source IP Address Input	SIP Contact Header
Enable Alt Routing Tel to IP	Disable
Alt Routing Tel to IP Mode	Both
Alt Routing Tel to IP Connectivity Method	ICMP Ping
Alt Routing Tel to IP Keep Alive Time	60
Alternative Routing Tone Duration [ms]	0
Source Manipulation Mode	FROM & PAI (after manipulation)
Max Allowed Packet Loss for Alt Routing [%]	20
Max Allowed Delay for Alt Routing [msec]	250

- Configure the parameters as required.
- Click **Submit** to apply your changes.

18.4.2 Configuring Outbound IP Routing Table

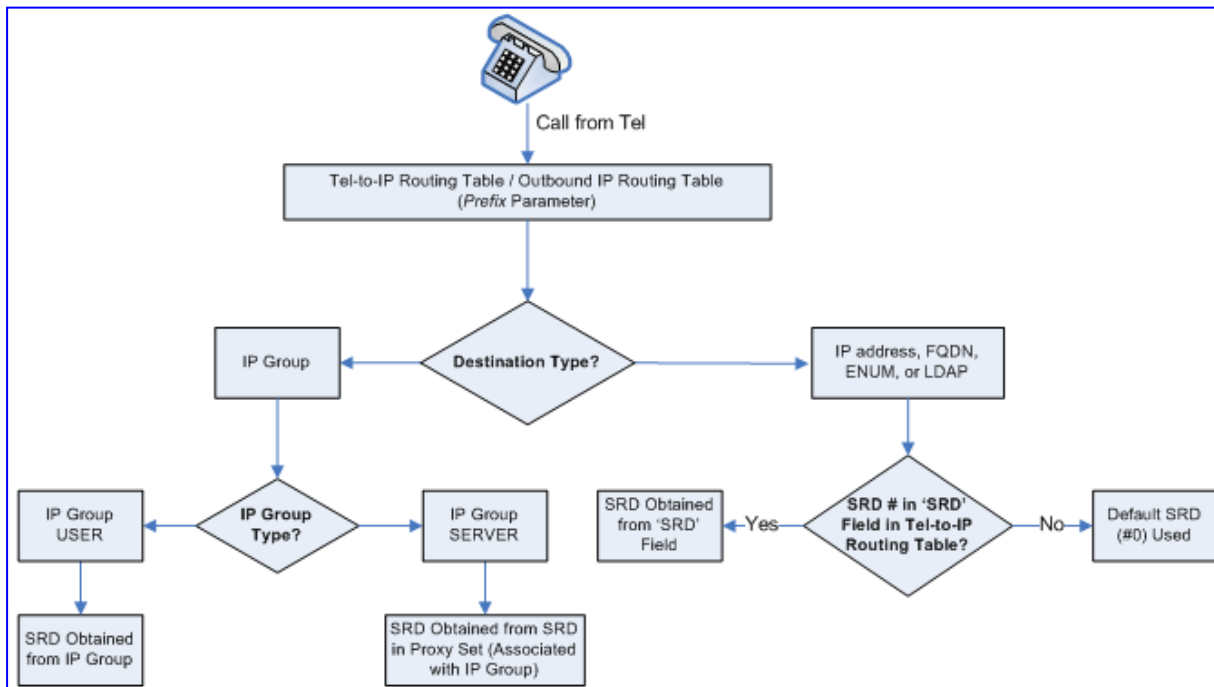
The Outbound IP Routing Table page allows you to configure up to 180 Tel-to-IP/outbound IP call routing rules. The device uses these rules to route calls from the Tel or IP to user-defined IP destinations.

The Outbound IP Routing Table 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:
 - Source IP Group (to which the call belongs)
 - Source and destination Request-URI host name prefix
 - Source Trunk Group (from where the call is received)
 - Source (calling) and destination (called) telephone number prefix and suffix
 - Source and destination Request-URI host name prefix
- **Destination:** 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' on page [177](#)
 - IP Group - the call is routed to the Proxy Set (IP address) or SRD associated with the IP Group (defined in 'Configuring IP Groups' on page [193](#)). If the device is configured with multiple SRDs, you can also indicate (in the table's 'Dest. SRD' field) the destination SRD for routing to one of the following destination types - IP address, FQDN, ENUM, or LDAP. If the SRD is not selected, then the default SRD—0—is used. In scenarios where routing is to an IP Group, the destination SRD is obtained from the SRD defined for that IP Group (in the IP Group table). The specified destination SRD determines the:
 - Destination SIP interface (SIP port and control IP interface) - important when using multiple SIP control VLANs
 - Media Realm (port and IP interface for media / RTP voice)
 - Other SRD-related interfaces and features on which the call is routed

Since each call must have a destination IP Group (even in cases where the destination type is not to an IP Group), in cases when the IP Group is not specified, the SRD's default IP Group is used (the first defined IP Group that belongs to the SRD).

Figure 18-11: Locating SRD



Notes: When using a proxy server, you do not need to configure this table unless you require one of the following:

- Fallback(alternative) routing if communication is lost with the proxy server.
- IP security, whereby the device routes only received calls whose source IP addresses are defined in this table. IP security is enabled using the SecureCallFromIP parameter.
- Filter Calls to IP feature: the device checks this table before a call is routed to the proxy server. However, if the number is not allowed, i.e., the number does not exist in the table or a Call Restriction (see below) routing rule is applied, the call is released.
- Obtain different SIP URI host names (per called number).
- Assign IP Profiles to calls.

For this table to take precedence over a proxy for routing calls, you need to set the parameter PreferRouteTable to 1. The device checks the 'Destination IP Address' field in this table for a match with the outgoing call; a proxy is used only if a match is not found.



In addition to basic outbound IP routing, supports the following features:

- **Least cost routing (LCR):** If the LCR feature is enabled, the device searches the routing table for matching routing rules and then selects the one with the lowest call cost. The call cost of the routing rule is done by assigning it a Cost Group. For configuring Cost Groups, see 'Least Cost Routing' on page 181. If two routing rules have identical costs, then the rule appearing higher up in the table (i.e., first-matched rule) is used. If a selected route is unavailable, the device uses the next least-cost routing rule. However, even if a matched rule is not assigned a Cost Group, the device can select it as the preferred route over other matched routing rules with Cost Groups, according to the settings of the LCR parameter, LCRDefaultCost (see 'Enabling the LCR Feature' on page 184).
- **Call forking:** If the Tel-to-IP Call Forking feature is enabled, the device can send a Tel call to multiple IP destinations. An incoming Tel call with multiple matched routing rules (e.g., all with the same source prefix numbers) can be sent (forked) to multiple IP destinations if the rules are defined with a Forking Group in the table. The call is established with the first IP destination that answers the call.
- **Call Restriction:** Rejects calls whose routing rule is associated with the destination IP address of 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 a specific call. To associate an alternative IP address to a called telephone number prefix, assign it with an additional entry (with a different IP address), or use an FQDN that resolves into two IP addresses. 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 more information on alternative routing, see 'Configuring Alternative Routing (Based on Connectivity and QoS' on page 340).
 - A defined Release Reason code is received (see 'Configuring Alternative Routing Reasons' on page 279).

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 279), 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. 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).

**Notes:**

- 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 Parameters' on page 732).

➤ **To configure outbound IP routing rules:**

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

	Src. IPGroupID	Src. Host Prefix	Dest Host Prefix	Src. Hunt Group ID	Dest. Phone Prefix	Source Phone Prefix
1	-1			*	10	100
2	-1			*	10	100
3	-1			*	20	*
4	-1			1	[5,7-9]	*
5	-1			*	00	*
6	2	domain.com		*	*	*
7	-1			*	100	*
8	-1			*	100	*
9	-1			*	100	*
10	-1					

Dest. IP Address	Port	Transport Type	Dest. IPGroup ID	Dest. SRD	IP Profile ID	Status	Charge Code	Cost Group ID	Forking Group
10.33.45.63		Not Configured	-1	-1	1	n/a		Weekend	-1
10.33.45.50		Not Configured	-1	-1	1	n/a		Weekend_B	-1
		Not Configured	1	-1	0	n/a		None	-1
domain.com		Not Configured	-1	-1	0	n/a		None	-1
0.0.0.0		Not Configured	-1	-1	0	n/a		None	-1
10.343.45.65		Not Configured	-1	-1	0	n/a		None	-1
10.33.45.68		Not Configured	-1	-1	0	n/a		None	1
10.33.45.67		Not Configured	-1	-1	0	n/a		None	2
domain.com		Not Configured	-1	-1	0	n/a		None	1
		Not Configured	-1					None	-1

The figure above displays the following outbound IP routing rules:

- **Rule 1 and Rule 2:** For both rules, the called phone number prefix is 10, the caller's phone number prefix is 100, and the call is assigned IP Profile ID 1. However, Rule 1 is assigned a cheaper Cost Group than Rule 2, and therefore, the call is sent to the destination IP address (10.33.45.63) associated with Rule 1.
 - **Rule 3:** 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 4:** If the called phone number prefix is 5, 7, 8, or 9 and the caller belongs to Trunk Group ID 1, the call is sent to domain.com.
 - **Rule 5:** For all callers (*), if the called phone number prefix is 00, the call is rejected (discarded).
 - **Rule 6:** If an incoming IP call pertaining to Source IP Group 2 with domain.com as source host prefix in its SIP Request-URI, the IP call is sent to IP address 10.33.45.65.
 - **Rule 7, Rule 8, and Rule 9:** For all callers (*), if the called phone number prefix is 100, the call is sent to Rule 7 and 9 (belonging to Forking Group "1"). If their destinations are unavailable and alternative routing is enabled, the call is sent to Rule 8 (Forking Group "2").
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 **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 470.

Table 18-13: Outbound IP Routing Table Parameters

Parameter	Description
Web/EMS: Tel to IP Routing Mode [RouteModeTel2IP]	<p>Determines whether to route received calls to an IP destination before or after manipulation of the destination number.</p> <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is not applicable if outbound proxy routing is used. ▪ For number manipulation, see 'Configuring Number Manipulation Tables' on page 254.
Web: Src. IPGroupID EMS: Source IP Group ID	<p>Defines the IP Group from where the incoming IP call is received. Typically, the IP Group of an incoming INVITE is determined according to the 'Inbound IP Routing Table'.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only for IP-to-IP routing. ▪ To denote all IP Groups, leave this field empty. ▪ If this IP Group has a Serving IP Group, then all calls from this IP Group are sent to the Serving IP Group. In such a scenario, this routing table is used only if the parameter PreferRouteTable is set to 1.
Web: Src. Host Prefix EMS: Source Host Prefix	<p>Defines the prefix of the SIP Request-URI host name in the From header of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ To denote any prefix, use the asterisk (*) symbol. ▪ This parameter is applicable only for IP-to-IP routing.
Web: Dest. Host Prefix EMS: Destination Host Prefix	<p>Defines the SIP Request-URI host name prefix of the incoming SIP INVITE message. If this routing rule is not required, leave the field empty.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ To denote any prefix, use the asterisk (*) symbol. ▪ This parameter is applicable only for IP-to-IP routing.
Web: Src. Trunk Group ID EMS: Source Trunk Group ID	<p>Defines the Trunk Group from where the call is received.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ To denote any Trunk Group, use the asterisk (*) symbol. ▪ This parameter is applicable only for the GW application.
Web: Dest. Phone Prefix EMS: Destination Phone Prefix	<p>Defines the prefix and/or suffix of the called (destination) telephone number. The suffix is enclosed in parenthesis after the suffix value. For example, [100-199](100,101,105) depicts a number that starts with 100 to 199 and ends with 100, 101 or 105. For a description of notations that you can use to represent single and multiple numbers (ranges), see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 767.</p> <p>The number can include up to 50 digits.</p> <p>Note: To denote any prefix, enter the asterisk (*) symbol.</p>

Parameter	Description
Web/EMS: Source Phone Prefix	<p>Defines the prefix and/or suffix of the calling (source) telephone number. For example, [100-199](100,101,105) depicts a number that starts with 100 to 199 and ends with 100, 101 or 105. For a description of notations that you can use to represent single and multiple numbers (ranges), see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 767.</p> <p>The number can include up to 50 digits.</p> <p>Note: To denote any prefix, enter the asterisk (*) symbol.</p>
<p>All calls matching all or any combination of the above characteristics are sent to the IP destination defined below.</p> <p>Note: For alternative routing, additional entries of the same prefix can be configured.</p>	
Web: Dest. IP Address EMS: Address	<p>Defines the 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.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 123). ▪ 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: <ul style="list-style-type: none"> ✓ "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	<p>Defines the destination port to where you want to route the call.</p>
Web/EMS: Transport Type	<p>Defines the transport layer type for sending the IP call:</p> <ul style="list-style-type: none"> ▪ [-1] Not Configured ▪ [0] UDP ▪ [1] TCP ▪ [2] TLS <p>Note: When set to Not Configured (-1), the transport type defined by the SIPTransportType parameter is used.</p>
Web: Dest IP Group ID EMS: Destination IP Group ID	<p>Defines the IP Group to where you want to route the call. The SIP INVITE message is sent to the IP address defined for the Proxy Set ID associated with the IP Group.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ If you select an IP Group, you do not need to configure a destination IP

Parameter	Description
	<p>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).</p> <ul style="list-style-type: none"> ▪ If the destination IP Group is of type USER, 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. ▪ If the parameter AlwaysUseRouteTable is set to 1 (see 'Configuring IP Groups' on page 193), 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 223). ▪ For defining Proxy Set ID's, see 'Configuring Proxy Sets Table' on page 198.
Dest SRD	<p>Defines the SRD to where you want to route the call. The actual destination is defined by the Proxy Set associated with the SRD. This allows you to route the call to a specific SIP Media Realm and SIP Interface.</p> <p>To configure SRD's, see Configuring SRD Table on page 189.</p>
IP Profile ID	<p>Associates an IP Profile ID with this IP destination call. This allows you to assign numerous configuration attributes (e.g., voice codes) per routing rule. To configure IP Profiles, see 'Configuring IP Profiles' on page 217.</p>
Status	<p>Displays the Quality of Service of the destination IP address:</p> <ul style="list-style-type: none"> ▪ "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)
Web/EMS: Charge Code	<p>Associates a Charge Code with the routing rule. To configure Charge Codes, see Configuring Charge Codes Table on page 314.</p> <p>Note: This parameter is applicable only to FXS interfaces.</p>
Cost Group ID	<p>Associates a Cost Group with the routing rule for determining the cost of the call. To configure Cost Groups, see 'Configuring Cost Groups' on page 186.</p>

Parameter	Description
Forking Group	<p>Defines a forking group ID for the routing rule. This enables forking of incoming Tel calls to two or more IP destinations. The device sends simultaneous INVITE messages and handles multiple SIP dialogs until one of the calls is answered. When a call is answered, the other calls are dropped. If all matched routing rules belong to the same Forking Group number, the device sends an INVITE to all the destinations belonging to this group and according to the following logic:</p> <ul style="list-style-type: none"> ▪ If matched routing rules belong to different Forking Groups, the device sends the call to the Forking Group of the first matched routing rule. If the call cannot be established with any of the destinations associated with this Forking Group and alternative routing is enabled, the device forks the call to the Forking Group of the next matched routing rules as long as the Forking Group is defined with a higher number than the previous Forking Group. For example: <ul style="list-style-type: none"> ▪ Table index entries 1 and 2 are defined with Forking Group "1", and index entries 3 and 4 with Forking Group "2": The device first sends the call according to index entries 1 and 2, and if unavailable and alternative routing is enabled, sends the call according to index entries 3 and 4. ▪ Table index entry 1 is defined with Forking Group "2", and index entries 2, 3, and 4 with Forking Group "1": The device sends the call according to index entry 1 only and ignores the other index entries even if the destination is unavailable and alternative routing is enabled. This is because the subsequent index entries are defined with a Forking Group number that is lower than that of index entry 1. ▪ Table index entry 1 is defined with Forking Group "1", index entry 2 with Forking Group "2", and index entries 3 and 4 with Forking Group "1": The device first sends the call according to index entries 1, 3, and 4 (all belonging to Forking Group "1"), and if the destination is unavailable and alternative routing is enabled, the device sends the call according to index entry 2. ▪ Table index entry 1 is defined with Forking Group "1", index entry 2 with Forking Group "3", index entry 3 with Forking Group "2", and index entry 4 with Forking Group "1": The device first sends the call according to index entries 1 and 4 (all belonging to Forking Group "1"), and if the destination is unavailable and alternative routing is enabled, the device sends the call according to index entry 2 (Forking Group "3"). Even if index entry 2 is unavailable and alternative routing is enabled, the device ignores index entry 3 because it belongs to a Forking Group that is lower than index entry 2. <p>Notes:</p> <ul style="list-style-type: none"> ▪ To enable Tel-to-IP call forking, you must set the 'Tel2IP Call Forking Mode' (<i>Tel2IPCallForkingMode</i>) parameter to Enable. ▪ You can implement Forking Groups when the destination is an LDAP server or a domain name using DNS. In such scenarios, the INVITE is sent to all the queried LDAP or resolved IP addresses respectively. You can also use LDAP routing rules with standard routing rules for Forking Groups.

18.4.3 Configuring Inbound IP Routing Table

The Inbound IP Routing Table page allows you to configure up to 24 inbound call routing rules:

- For IP-to-IP routing: identifying IP-to-IP calls and assigning them to IP Groups (referred to as Source IP Groups). These IP-to-IP calls, now pertaining to an IP Group, can later be routed to an outbound destination IP Group (see [Configuring Outbound IP Routing Table](#) on page 269).
- For IP-to-Tel routing: routing incoming IP calls to Trunk Groups. The specific channel pertaining to the Trunk Group to which the call is routed is determined according to the Trunk Group's channel selection mode. The channel selection mode can be defined per Trunk Group (see 'Configuring Trunk Group Settings' on page 251), or for all Trunk 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:
 - Source and destination Request-URI host name prefix
 - Source (calling) and destination (called) telephone number prefix and suffix
 - Source IP address (from where the call is received)
- **Destination:** user-defined destination. If the call matches the characteristics, the device routes the call to the defined destination:
 - Trunk Group
 - Source IP Group



Notes:

- When a call release reason (defined in 'Configuring Reasons for Alternative Routing' on page 279) is received for a specific IP-to-Tel call, an alternative Trunk 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 Trunk Group ID.
- You can also configure the Inbound IP Routing Table using the *ini* file table parameter PSTNPrefix (see 'Number Manipulation Parameters' on page 732).

➤ To configure inbound IP routing rules:

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

Figure 18-12: Inbound IP Routing Table

Routing Index		1-12		IP To Tel Routing Mode		Route calls before manipulation	
Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IPGroup ID
1		1x	*		1	2	-1
2		[501-502]	101		2	1	
3	domain.com	*	*		3		
4		*	*	10.13.64.5	-1		4

The previous figure displays the following configured routing rules:

- **Rule 1:** If the incoming IP call destination phone prefix is between 10 and 19, the call is assigned settings configured for IP Profile ID 2 and routed to Trunk Group ID 1.
 - **Rule 2:** If the incoming IP call destination phone prefix is between 501 and 502, and source phone prefix is 101, the call is assigned settings configured for IP Profile ID 1 and routed to Trunk Group ID 2.
 - **Rule 3:** If the incoming IP call has a From URI host prefix as domain.com, the call is routed to Trunk Group ID 3.
 - **Rule 4:** If the incoming IP call has IP address 10.13.64.5 in the INVITE's Contact header, the call is identified as an IP-to-IP call and assigned to Source IP Group 4. This call is routed according to the outbound IP routing rules for this Source IP Group configured in the Outbound IP Routing Table'.
2. 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 **Submit** to apply your changes.
 5. To save the changes so they are available after a power failure, see 'Saving Configuration' on page [470](#).

Table 18-14: Inbound IP 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 254). <ul style="list-style-type: none"> ▪ [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: <ul style="list-style-type: none"> ▪ 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	Defines the prefix or suffix of the called (destined) telephone number. For example, [100-199](100,101,105) depicts a number that starts with 100 to 199 and ends with 100, 101 or 105. For a description of notations that you can use to represent single and multiple numbers (ranges), see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 767 . The prefix can include up to 49 digits.
Source Phone Prefix	Defines the prefix or suffix of the calling (source) telephone number. For example, [100-199](100,101,105) depicts a number that starts with 100 to 199 and ends with 100, 101 or 105. For a description of notations that you can use to represent single and multiple numbers (ranges), see 'Dialing Plan Notation for Routing and Manipulation Tables' on page 767 . The prefix can include up to 49 digits.

Parameter	Description
Source IP Address	<p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ You can configure from where the source IP address is obtained, using the parameter SourceIPAddressInput. ▪ The source IP address can include the following wildcards: <ul style="list-style-type: none"> ✓ "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.
<p>Calls matching all or any combination of the above characteristics are sent to the Trunk Group ID or assigned to the source IP Group for IP-to-IP routing defined below.</p> <p>Note: For alternative routing, additional entries of the same characteristics can be configured.</p>	
Trunk Group ID	<p>For IP-to-Tel calls: The Trunk Group to which the incoming SIP call is assigned if it matches all or any combination of the parameters described above.</p> <p>For IP-to-IP calls: Identifies the call as an IP-to-IP call when this parameter is set to -1.</p>
IP Profile ID	The IP Profile (configured in 'Configuring IP Profiles' on page 217) to assign to the call.
Source IP Group ID	<p>For IP-to-Tel calls: 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 223).</p> <p>For IP-to-IP calls: The IP Group you want to assign the incoming IP call. This IP Group can later be used for outbound IP routing and as the 'Serving IP Group' in the Account table for obtaining authentication user name/password for this call (see Configuring Account Table on page 223).</p>

18.4.4 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 searches for 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 Trunk Group is provided. For defining an alternative Trunk Group, see 'Configuring Inbound IP Routing Table' on page 277. 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 Outbound IP Routing Table' on page 269. 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 Parameters' on page 732).

➤ **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 18-13: Reasons for Alternative Routing Page

IP to Tel Reasons	
Reason 1	▼
Reason 2	▼
Reason 3	▼
Reason 4	▼
Reason 5	▼
Tel to IP Reasons	
Reason 1	▼
Reason 2	▼
Reason 3	▼
Reason 4	▼
Reason 5	▼

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 **Submit** to apply your changes.

18.4.5 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 Trunk Group), or when an appropriate rule for routing the call to a Trunk 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.

18.4.6 Configuring Call Forward upon Busy Trunk

The Forward on Busy Trunk Destination page allows you to configure forwarding (call redirection) of IP-to-Tel calls to a different (alternative) IP destination, using SIP 3xx responses upon the following scenarios:

- For digital interfaces: If a Trunk Group has no free channels (i.e., "busy" Trunk Group).
- For analog interfaces: if an unavailable FXS/FXO Trunk Group exists. This feature can be used, for example, to forward the call to another FXS/FXO device.

This alternative destination is configured per Trunk 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 one of the following reasons (included in the SIP Diversion header of 3xx messages) exists:

- For digital interfaces: "out-of-service" - all trunks are unavailable/disconnected
- "unavailable":
 - For digital interfaces: All trunks are busy or unavailable
 - For analog interfaces: All FXS/FXO lines pertaining to a Trunk Group are busy or unavailable



Note: You can also configure the Forward on Busy Trunk Destination table using the *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 18-14: 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 Trunk Group ID 1 to destination IP address 10.13.5.67 if the conditions mentioned earlier exist.

2. Configure the table as required, and then click **Submit** to apply your changes.
3. To save the changes so they are available after a power fail, see 'Saving Configuration' on page 470.

18.5 DTMF and Supplementary

This section describes configuration of the DTMF and supplementary parameters.

18.5.1 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 529.

➤ **To configure the DTMF and dialing parameters:**

1. Open the DTMF & Dialing page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **DTMF & Supplementary** submenu > **DTMF & Dialing**).

Max Digits In Phone Num	<input type="text" value="30"/>
Inter Digit Timeout [sec]	<input type="text" value="4"/>
Declare RFC 2833 in SDP	<input type="text" value="Yes"/>
1st Tx DTMF Option	<input type="text" value="RFC 2833"/>
2nd Tx DTMF Option	<input type="text"/>
RFC 2833 Payload Type	<input type="text" value="96"/>
Hook-Flash Option	<input type="text" value="Not Supported"/>
Digit Mapping Rules	<input type="text"/>
Dial Plan Index	<input type="text" value="-1"/>
Dial Tone Duration [sec]	<input type="text" value="16"/>
Hotline Dial Tone Duration [sec]	<input type="text" value="16"/>
Enable Special Digits	<input type="text" value="Disable"/>
Dial Plan Index	<input type="text" value="-1"/>
Min Routing Overlap Digits	<input type="text" value="1"/>
ISDN Overlap IP to Tel Dialing	<input type="text" value="Disable"/>
Default Destination Number	<input type="text" value="1000"/>
Special Digit Representation	<input type="text" value="Special"/>

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

18.5.2 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 529.

The procedure below describes how to access the Supplementary Services page and configure the supplementary services parameters. In addition to this, you can also refer to the following specific services configuration:

- Call hold and retrieve - see 'Call Hold and Retrieve' on page 285
- BRI suspend-resume - see BRI Suspend and Resume on page 287
- Consultation - see Consultation Feature on page 287
- Call transfer - see 'Call Transfer' on page 288
- Call forward - see 'Call Forward' on page 289
- Call waiting - see Call Waiting on page 292
- Message waiting indication (MWI)- see 'Message Waiting Indication' on page 293
- Caller ID - see Caller ID on page 294
- Three-way conferencing - see Three-Way Conferencing on page 297
- Emergency 911 calls - see Emergency E911 Phone Number Services on page 298
- Multilevel Precedence and Preemption (MLPP) - see 'Multilevel Precedence and Preemption' on page 304
- Denial of collect calls - see Denial of Collect Calls on page 307



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.

➤ **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**).

Enable Hold	Enable	▼
Enable Hold to ISDN	Disable	▼
Hold Format	0.0.0.0	▼
Held Timeout	-1	
Call Hold Reminder Ring Timeout	30	
Enable Transfer	Enable	▼
Transfer Prefix		
Enable Call Forward	Enable	▼
Enable Call Waiting	Enable	▼
Number of Call Waiting Indications	2	
Time Between Call Waiting Indications	10	
Time Before Waiting Indications	0	
Waiting Beep Duration	300	
Enable Caller ID	Disable	▼
Caller ID Type	Standard Bellcore	▼
Hook-Flash Code		
Flash Keys Sequence Style	0	
Flash Keys Sequence Timeout	2000	
⚡ Max 3 Way Conference on Board Calls	2	
⚡ Non Allocatable Ports	0	
Enable NRT Subscription	Disable	▼
AS Subscribe IPGroupID	-1	
NRT Subscribe Retry Time	120	
Call Forward Ring Tone ID	1	
▼ MWI Parameters		
Enable MWI	Disable	▼
MWI Analog Lamp	Disable	▼
MWI Display	Disable	▼
Subscribe to MWI	No	▼
MWI Server Transport Type	Not Configured	▼
MWI Server IP Address		
MWI Subscribe Expiration Time	7200	
MWI Subscribe Retry Time	120	
Stutter Tone Duration	2000	
▼ Conference		
⚡ Enable 3-Way Conference	Disable	▼
Establish Conference Code	!	
Conference ID	conf	
Three Way Conference Mode	AudioCodes Media Server	▼
▼ MLPP		
Call Priority Mode	Disable	▼
MLPP Diffserv	50	
Precedence Ringing Type	-1	
▼ BRI to SIP Supplementary Services Codes		
Call Forward Unconditional		
Call Forward Unconditional Deactivation		
Call Forward on Busy		
Call Forward on Busy Deactivation		
Call Forward on No Reply		
Call Forward on No Reply Deactivation		
▼ Transfer		
Blind		

2. Configure the parameters as required.
3. Click **Submit** to apply your changes, or click the **Subscribe to MWI** or **Unsubscribe to MWI** buttons to save your changes and to subscribe / unsubscribe to the MWI server.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

18.5.2.1 Call Hold and Retrieve

Initiating Call Hold and Retrieve:

- Active calls can be put on-hold by pressing the phone's hook-flash button.
- The party that initiates the hold is called the *holding* party; the other party is called the *held* party.
- After a successful Hold, the holding party hears a Dial tone (HELD_TONE defined in the device's Call Progress Tones file).
- Call retrieve can be performed only by the holding party while the call is held and active.
- The holding party performs the retrieve by pressing the telephone's hook-flash button.
- After a successful retrieve, the voice is connected again.
- Hold is performed by sending a Re-INVITE message with IP address 0.0.0.0 or a=sendonly in the SDP according to the parameter HoldFormat.
- The hold and retrieve functionalities are implemented by Re-INVITE messages. The IP address 0.0.0.0 as the connection IP address or the string 'a=inactive' in the received Re-INVITE SDP cause the device to enter Hold state and to play the Held tone (configured in the device) to the PBX/PSTN. If the string 'a=sendonly' is received in the SDP message, the device stops sending RTP packets, but continues to listen to the incoming RTP packets. Usually, the remote party plays, in this scenario, Music on Hold (MOH) and the device forwards the MOH to the held party.

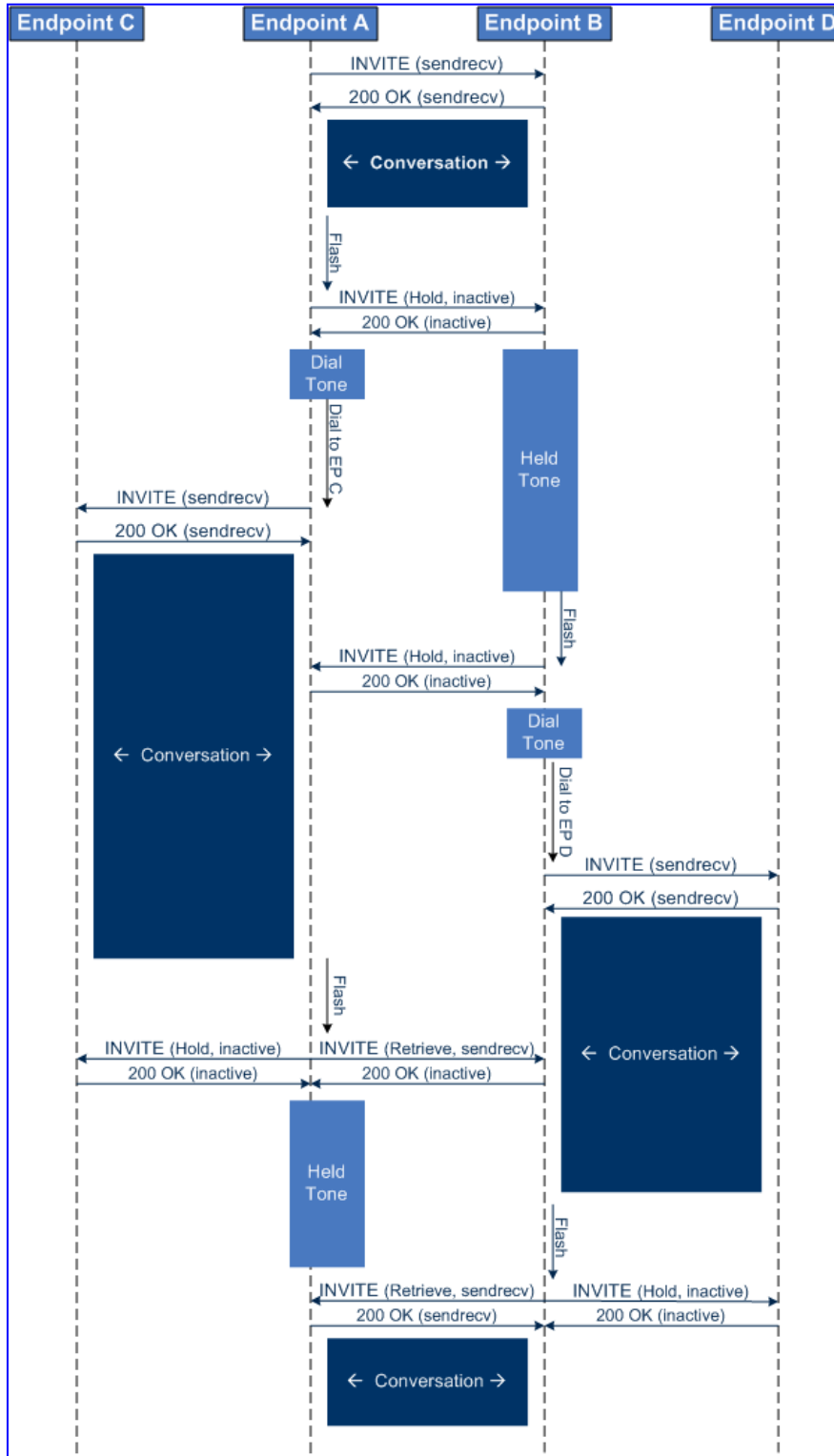
Receiving Hold/Retrieve:

- When an active call receives a Re-INVITE message with either the IP address 0.0.0.0 or the 'inactive' string in SDP, the device stops sending RTP and plays a local Held tone.
- When an active call receives a Re-INVITE message with the 'sendonly' string in SDP, the device stops sending RTP and listens to the remote party. In this mode, it is expected that on-hold music (or any other hold tone) is played (over IP) by the remote party.

You can also configure the device to keep a call on-hold for a user-defined time after which the call is disconnected, using the HeldTimeout parameter.

The device also supports "double call hold" for FXS interfaces where the called party, which has been placed on-hold by the calling party, can then place the calling party on hold as well and make a call to another destination. The flowchart below provides an example of this type of call hold:

Figure 18-15: 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).

18.5.2.2 BRI Suspend and Resume

The device supports call suspend and resume services initiated by ISDN BRI phones connected to the device. During an ongoing call, the BRI phone user can suspend the call by typically pressing the phone's "P" button or a sequence of keys (depending on the phone), and then on-hooking the handset. To resume the call, the phone user typically presses the same keys or button again and then off-hooks the phone. During the suspended state, the device plays a Howler tone to the remote party. This service is also supported when instead of pressing the call park button(s), the phone cable is disconnected (suspending the call) and then reconnected again (resuming the call).

If the phone user does not resume the call within a user-defined interval (configured using the HeldTimeout parameter), the device releases the call.



Note: Only one call can be suspended per trunk. If another suspend request is received from a BRI phone while there is already a suspended call (even if done by another BRI phone connected to the same trunk), the device rejects this suspend request.

18.5.2.3 Consultation Feature

The device's Consultation feature allows you to place one number on hold and make a second call to another party.

- After holding a call (by pressing hook-flash), the holding party hears a dial tone and can then initiate a new call, which is called a Consultation call.
- While hearing a dial tone, or when dialing to the new destination (before dialing is complete), the user can retrieve the held call by pressing hook-flash.
- The held call can't be retrieved while Ringback tone is heard.
- After the Consultation call is connected, the user can toggle between the held and active call by pressing the hook-flash key.



Note: The Consultation feature is applicable only to FXS interfaces.

18.5.2.4 Call Transfer

The device supports the following call transfer types:

- Consultation Transfer (see 'Consultation Call Transfer' on page 288)
- Blind Transfer (see 'Blind Call Transfer' on page 289)



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.

18.5.2.4.1 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.

The device also supports attended (consultation) call transfer for BRI phones (user side) connected to the device and using the Euro ISDN protocol. BRI call transfer is according to ETSI TS 183 036, Section G.2 (Explicit Communication Transfer – ECT). Call transfer is enabled using the EnableTransfer and EnableHoldtoISDN parameters.

The Explicit Call Transfer (ECT, according to ETS-300-367, 368, 369) supplementary service is supported for BRI and PRI trunks. This service provides the served user who has two calls to ask the network to connect these two calls together and release its connection to both parties. The two calls can be incoming or outgoing calls. This service is similar to NI2 Two B-Channel Transfer (TBCT) Supplementary Service. The main difference is that in ECT one of the calls must be in HELD state. The ECT standard defines two methods - Implicit and Explicit. In implicit method, the two calls must be on the same trunk. BRI uses the implicit mechanism, and PRI the explicit mechanism.

18.5.2.4.2 Consultation Transfer for QSIG Path Replacement

The device can interwork consultation call transfer requests for ISDN QSIG-to-IP calls. When the device receives a request for a consultation call transfer from the PBX, the device sends a SIP REFER message with a Replaces header to the SIP UA to transfer it to another SIP UA. Once the two SIP UA parties are successfully connected, the device requests the PBX to disconnect the ISDN call, thereby freeing resources on the PBX.

For example, assume legacy PBX user "A" has two established calls connected through the device – one with remote SIP UA "B" and the other with SIP UA "C". In this scenario, user "A" initiates a consultation call transfer to connect "B" with "C". The device receives the consultation call transfer request from the PBX and then connects "B" with "C", by sending "B" a REFER message with a Replaces header (i.e., replace caller "A" with "C"). Upon receipt of a SIP NOTIFY 200 message in response to the REFER, the device sends a Q.931 DISCONNECT messages to the PBX, notifying the PBX that it can disconnect the ISDN calls (of user "A").

This feature is enabled by the QSIGPathReplacementMode parameter.

18.5.2.4.3 Blind Call Transfer

Blind call transfer is done (using SIP REFER messages) after a call is established between call parties A and B, and party A decides to immediately transfer the call to C without speaking to C. The result of the transfer is a call between B and C (similar to consultation transfer, but skipping the consultation stage).



Note: Currently, the device does not support blind transfer for BRI interfaces.

18.5.2.5 Call Forward

For digital interfaces: The device supports Call Deflection (ETS-300-207-1) for Euro ISDN and QSIG (ETSI TS 102 393) for Network and User sides, which provides IP-ISDN interworking of call forwarding (call diversion) when the device receives a SIP 302 response.

Call forward performed by the SIP side: Upon receipt of a Facility message with Call Rerouting IE from the PSTN, the device initiates a SIP transfer process by sending a SIP 302 (including the Call Rerouting destination number) to the IP in response to the remote SIP entity's INVITE message. The device then responds with a Disconnect message to the PSTN side.

Call forward performed by the PSTN side: When the device sends the INVITE message to the remote SIP entity and receives a SIP 302 response, the device sends a Facility message with the same IE mentioned above to the PSTN, and waits for the PSTN side to disconnect the call. This is configured using the CallReroutingMode.

For analog interfaces: The following methods of call forwarding are supported:

- Immediate: incoming call is forwarded immediately and unconditionally.
- Busy: incoming call is forwarded if the endpoint is busy.
- No Reply: incoming call is forwarded if it isn't answered for a specified time.
- On Busy or No Reply: incoming call is forwarded if the port is busy or when calls are not answered after a specified time.
- Do Not Disturb: immediately reject incoming calls. Upon receiving a call for a Do Not Disturb, the 603 Decline SIP response code is sent.

Three forms of forwarding parties are available:

- Served party: party configured to forward the call (FXS device).
- Originating party: party that initiates the first call (FXS or FXO device).
- Diverted party: new destination of the forwarded call (FXS or FXO device).

The served party (FXS interface) can be configured through the Web interface (see Configuring Call Forward on page 319) or ini file to activate one of the call forward modes. These modes are configurable per endpoint.

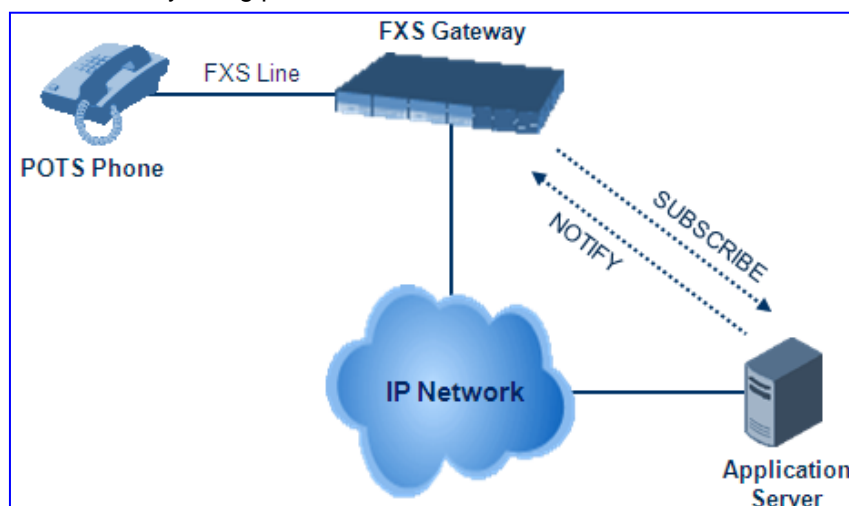


Notes:

- 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.

18.5.2.5.1 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.



The device generates a Call Forward Reminder ring burst to the FXS endpoint each time it receives a SIP NOTIFY message with a "reminder ring" xml body. The NOTIFY request is sent from the Application Server to the device each time the Application Server forwards an incoming call. The service is cancelled when an UNSUBSCRIBE request is sent from the device, or when the Subscription time expires.

The Reminder Ring tone can be defined by using the parameter CallForwardRingToneID, which points to a ring tone defined in the Call Progress Tone file.

The following parameters are used to configure this feature:

- EnableNRTSubscription
- ASSubscribeIPGroupID
- NRTSubscribeRetryTime
- CallForwardRingToneID

18.5.2.5.2 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/simserv+xml"
- Message body is the XML body and contains the "dial-tone-pattern" set to "special-condition-tone" (<ss:dial-tone-pattern>special-condition-tone</ss:dial-tone-pattern>), which is the special tone indication.

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/simserv+xml"
- Message body is the XML body containing the "dial-tone-pattern" set to "standard-condition-tone" (<ss:dial-tone-pattern>standard-condition-tone</ss:dial-tone-pattern>), which is the regular dial tone indication.

Therefore, the special dial tone is valid until another SIP NOTIFY is received that instructs otherwise (as described above).



Note: if the MWI service is active, the MWI dial tone overrides this special Call Forward dial tone

18.5.2.5.3 BRI Call Forwarding

The device supports call forwarding (CF) services initiated by ISDN Basic BRI phones connected to it. Upon receipt of an ISDN Facility message for call forward from the BRI phone, the device sends a SIP INVITE to the softswitch with a user-defined code in the SIP To header, representing the reason for the call forward.

The codes for the call forward can be defined using the following parameters:

- SuppServCodeCFU - Call Forward Unconditional
- SuppServCodeCFUDeact - Call Forward Unconditional Deactivation
- SuppServCodeCFB - Call Forward on Busy
- SuppServCodeCFBDeact - Call Forward on Busy Deactivation
- SuppServCodeCFNR - Call Forward on No Reply
- SuppServCodeCFNRDeact - Call Forward on No Reply Deactivation



Note: These codes must be defined according to the settings of the softswitch (i.e., the softswitch must recognize them).

Below is an example of an INVITE message sent by the device indicating an unconditional call forward (“*72”) to extension number 100. This code is defined using the SuppServCodeCFU parameter.

```
INVITE sip:*72100@10.33.8.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.5:5060;branch=z9hG4bKWDSUKUHFEXQSVUUVJGM
From: <sip:400@10.33.2.5;user=phone>;tag=DUOROSXSQYJLLNBFRTG
To: <sip:*72100@10.33.8.53;user=phone>
Call-ID: GMNOVQRRXUUCYCQSFQHS@10.33.2.5
CSeq: 1 INVITE
Contact: <sip:400@10.33.2.5:5060>
Supported: em,100rel,timer,replaces
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE
User-Agent: Sip Message Generator V1.0.0.5
User-to-User: 31323334;pd=4
Content-Type: application/sdp
Content-Length: 155
```

18.5.2.6 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 FirstCallWaitingToneID parameter).
4. To configure the Call Waiting indication tone cadence, modify the following parameters: NumberOfWaitingIndications, WaitingBeepDuration and TimeBetweenWaitingIndications.
5. To configure a delay interval before a Call Waiting Indication is played to the currently busy port, use the parameter TimeBeforeWaitingIndication. This enables the caller to hang up before disturbing the called party with Call Waiting Indications. Applicable only to FXS modules.

Both the calling and called sides are supported by FXS interfaces; FXO interfaces support only the calling side.

To indicate Call Waiting, the device sends a 182 Call Queued response. The device identifies Call Waiting when a 182 Call Queued response is received.



Note: The Call Waiting feature is applicable only to FXS/FXO interfaces.

18.5.2.7 Message Waiting Indication

The device supports Message Waiting Indication (MWI) according to IETF RFC 3842, including SUBSCRIBE (to an MWI server).



Note: For more information on IP voice mail configuration, refer to the *IP Voice Mail CPE Configuration Guide*.

For analog interfaces: The FXS device can accept an MWI NOTIFY message that indicates waiting messages or that the MWI is cleared. Users are informed of these messages by a stutter dial tone. The stutter and confirmation tones are defined in the CPT file (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, or MWISubscribeIPGroupID and ProxySet
- MWIAnalogLamp
- MWIDisplay
- StutterToneDuration
- EnableMWISubscription
- MWIExpirationTime
- SubscribeRetryTime
- SubscriptionMode
- CallerIDType (determines the standard for detection of MWI signals)
- ETSIVMWITypeOneStandard
- BellcoreVMWITypeOneStandard
- VoiceMailInterface
- EnableVMURI

The device supports the following MWI features for its digital PSTN interfaces:

- For BRI interfaces: This feature provides support for MWI on BRI phones connected to the device and using the Euro ISDN BRI variant. When this feature is activated and a voice mail message is recorded to the mail box of a BRI extension, the softswitch sends a notification to the device. In turn, the device notifies the BRI extension and a red light flashes on the BRI extension's phone. Once the voice message is retrieved, the MWI light on the BRI extension turns off. This feature is configured by setting the VoiceMailInterface parameter to 8 ("ETSI") and enabled by the EnableMWI parameter.
- Euro-ISDN MWI: The device supports Euro-ISDN MWI for IP-to-Tel calls. The device interworks SIP MWI NOTIFY messages to Euro-ISDN Facility information element (IE) MWI messages. This is supported by setting the VoiceMailInterface parameter to 8.

- QSIG MWI: The device also supports the interworking of QSIG MWI to IP (in addition to interworking of SIP MWI NOTIFY to QSIG Facility MWI messages). This provides interworking between an ISDN PBX with voicemail capabilities and a softswitch, which requires information on the number of messages waiting for a specific user. This support is configured using the MWIInterrogationType parameter, which determines the device's handling of MWI Interrogation messages. The process for sending the MWI status upon request from a softswitch is as follows:
 1. The softswitch sends a SIP SUBSCRIBE message to the device.
 2. The device responds by sending an empty SIP NOTIFY to the softswitch, and then sending an ISDN Setup message with Facility IE containing an MWI Interrogation request to the PBX.
 3. The PBX responds by sending to the device an ISDN Connect message containing Facility IE with an MWI Interrogation result, which includes the number of voice messages waiting for the specific user.
 4. The device sends another SIP NOTIFY to the softswitch, containing this MWI information.
 5. The SIP NOTIFY messages are sent to the IP Group defined by the NotificationIPGroupID parameter.

In addition, when a change in the status occurs (e.g., a new voice message is waiting or the user has retrieved a message from the voice mail), the PBX initiates an ISDN Setup message with Facility IE containing an MWI Activate request, which includes the new number of voice messages waiting for the user. The device forwards this information to the softswitch by sending a SIP NOTIFY.

Depending on the PBX support, the MWIInterrogationType parameter can be configured to handle these MWI Interrogation messages in different ways. For example, some PBXs support only the MWI Activate request (and not MWI Interrogation request). Some support both these requests. Therefore, the device can be configured to disable this feature, or enable it with one of the following support:

- Responds to MWI Activate requests from the PBX by sending SIP NOTIFY MWI messages (i.e., does not send MWI Interrogation messages).
- Send MWI Interrogation message, but don't use its result. Instead, wait for MWI Activate requests from the PBX.
- Send MWI Interrogation message, use its result, and use the MWI Activate requests.

18.5.2.8 Caller ID

This section discusses the device's Caller ID support.



Note: The Caller ID feature is applicable only to FXS/FXO interfaces.

18.5.2.8.1 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.
- `AnalogCallerIDTimingMode`: determines the time period when a caller ID signal is generated (FXS only). By default, the caller ID is generated between the first two rings.
- `PolarityReversalType`: some Caller ID signals use reversal polarity and/or wink signals. In these scenarios, it is recommended to set `PolarityReversalType` to 1 (Hard) (FXS only).
- The Caller ID interworking can be changed using the parameters `UseSourceNumberAsDisplayName` and `UseDisplayNameAsSourceNumber`.

18.5.2.8.2 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**.

18.5.2.8.3 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.

18.5.2.9 Three-Way Conferencing

The device supports three-way conference calls. These conference calls can also occur simultaneously. The device supports the following conference modes (configured by the parameter `3WayConferenceMode`):

- **Conferencing 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 sets up the call conference using its IP media channels. These channels are obtained from the IP media module (i.e., MPM module). Note that the MPM module(s) must be installed to support three-way conferencing. The device supports up to five simultaneous, on-board, three-way conference calls. For this mode, the `3WayConferenceMode` parameter is set to 2.

**Notes:**

- Three-way conferencing using an external conference server is supported only by FXS interfaces.
- The on-board, three-way conference mode is not supported by Mediant 600.
- Instead of using the flash-hook button to establish a three-way conference call, you can dial a user-defined hook-flash code (e.g., `**1`), configured by the `HookFlashCode` parameter.
- Three-way conferencing is applicable only to FXS and BRI interfaces. Three-way conferencing support for the BRI phones connected to the device complies with ETS 300 185.
-

The 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").

To configure three-way conferencing:

- Enable3WayConference
- ConferenceCode = '!' (default, which is the hook flash button)
- HookFlashCode
- 3WayConferenceMode (conference mode)
- FlashKeysSequenceStyle = 1 or 2 (makes a three-way call conference using the Flash button + 3)

18.5.2.10 Emergency E911 Phone Number Services

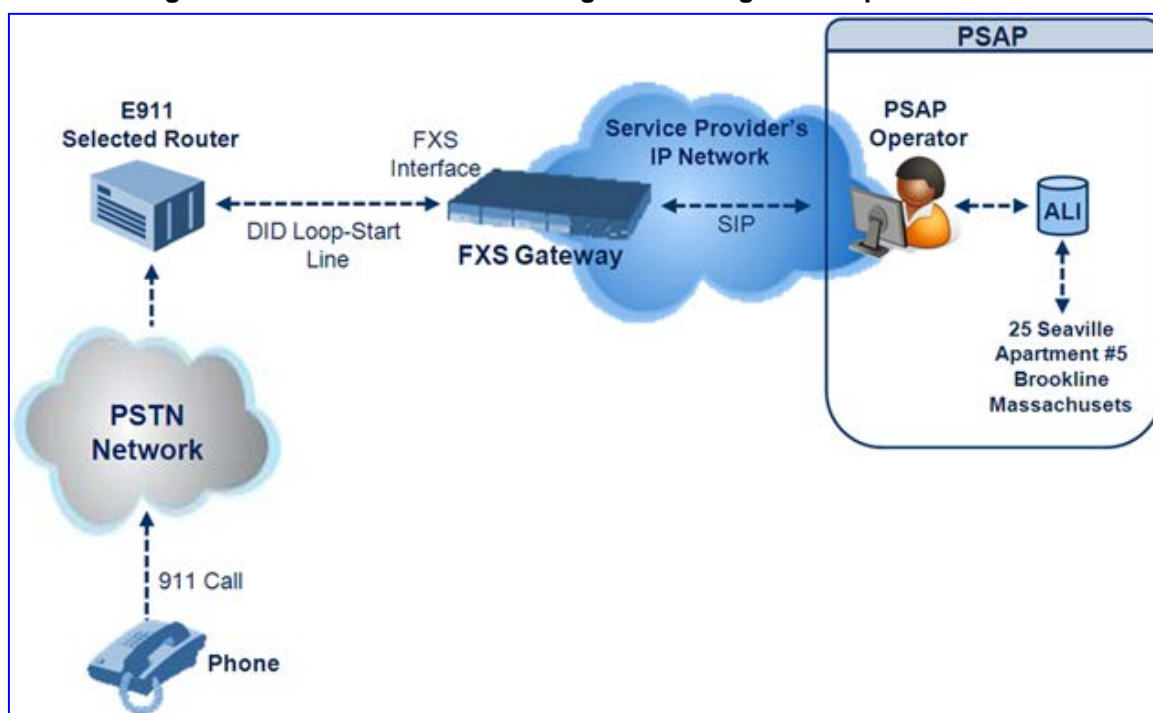
The device supports emergency phone number services. The device supports the North American emergency telephone number system known as Enhanced 911 (E911), according to the TR-TSY-000350 and Bellcore's GR-350-Jun2003 standards. The E911 emergency system automatically associates a physical address with the calling party's telephone number, and routes the call to the most appropriate (closest) Public Safety Answering Point (PSAP), allowing the PSAP to quickly dispatch emergency response (e.g., police) to the caller's location.

Typically, the dialed emergency number is routed to the appropriate PSAP by the telephone company's switch, known as a 911 Selective Router (or E911 tandem switch). If the PSAP receives calls from the telephone company on old-style digital trunks, they are specially formatted Multi-Frequency (MF) trunks that pass only the calling party's number (known as Automatic Number Identification - ANI). Once the PSAP receives the call, it searches for the physical address that is associated with the calling party's telephone number (in the Automatic Location Identification database - ALI).

18.5.2.10.1 FXS Device Emulating PSAP using DID Loop-Start Lines

The FXS device can be configured to emulate PSAP (using DID loop start lines), according to the Telcordia GR-350-CORE specification.

Figure 18-16: FXS Device Emulating PSAP using DID Loop-Start Lines



The call flow of an E911 call to the PSAP is as follows:

1. The E911 tandem switch seizes the line.
2. The FXS device detects the line seize, and then generates a wink signal (nominal 250 msec). The wink can be delayed by configuring the parameter `DelayBeforeDIDWink` to 200 (for 200 msec or a higher value).
3. The switch detects the wink and then sends the MF Spill digits with ANI and (optional) Pseudo-ANI (P ANI).
4. The FXS device collects the MF digits, and then sends a SIP INVITE message to the PSAP with all collected MF digits in the SIP From header as one string.
5. The FXS device generates a mid-call wink signal (two subsequent polarity reversals) toward the E911 tandem switch upon either detection of an RFC 2833 "hookflash" telephony event, or if a SIP INFO message with a "hooflash" body is received from the PSAP (see the example below). The duration of this "flashhook" wink signal is configured using the parameter `FlashHookPeriod` (usually 500 msec). Usually the wink signal is followed by DTMF digits sent by PSAP to perform call transfer. Another way to perform the call transfer is to use SIP REFER messages, as described below.
6. The FXS device supports call transfer initiated by the PSAP. If it receives a SIP REFER message with the Refer-To URI host part containing an IP address that is equal to the device's IP address, the FXS device generates a 500-msec wink signal (double polarity reversals), and then (after a user-defined interval configured by the parameter `WaitForDialTime`), plays DTMF digits according to the transfer number received in the SIP Refer-To header URI userpart.
7. When the call is answered by the PSAP operator, the PSAP sends a SIP 200 OK to the FXS device, and the FXS device then generates a polarity reversal signal to the E911 switch.
8. After the call is disconnected by the PSAP, the PSAP sends a SIP BYE to the FXS device, and the FXS device reverses the polarity of the line toward the tandem switch.

The following parameters need to be configured:

- `EnableDIDWink` = 1
- `EnableReversalPolarity` = 1
- `PolarityReversalType` = 1
- `FlashHookPeriod` = 500 (for 500 msec "hookflash" mid-call Wink)
- `WinkTime` = 250 (for 250 msec signalling Wink generated by the FXS device after it detects the line seizure)
- `EnableTransfer` = 1 (for call transfer)
- `LineTransferMode` = 1 (for call transfer)
- `WaitforDialTime` = 1000 (for call transfer)
- `SwapTEI2IPCalled&CallingNumbers` = 1
- `DTMFDetectorEnable` = 0
- `MFR1DetectorEnable` = 1
- `DelayBeforeDIDWink` = 200 (for 200 msec) - can be configured in the range from 0 (default) to 1000.



Note: Modification of the `WinkTime` and `FlashHookPeriod` parameters require a device reset.

The outgoing SIP INVITE message contains the following headers:

```
INVITE sip:Line@DomainName
From: <sip:*81977820#@sipgw>;tag=1c143
To: <sip:Line@DomainName>
```

Where:

- Line = as configured in the Endpoint Phone Number Table.
- SipGtw = configured using the SIPGatewayName parameter.
- From header/user part = calling party number as received from the MF spill.

The ANI and the pseudo-ANI numbers are sent to the PSAP either in the From and/or P-AssertedID SIP header.

Typically, the MF spills are sent from the E911 tandem switch to the PSAP, as shown in the table below:

Table 18-15: Dialed MF Digits Sent to PSAP

Digits of Calling Number	Dialed MF Digits
8 digits "nnnnnnnn" (ANI)	"KPnnnnnnnnST"
12 digits "nnnnnnnnnnnn" (ANI)	"KPnnnnnnnnnnnnSTP"
12 digits ANI and 10 digits PANI	"KPnnnnnnnnnnnnSTKPmmmmmmmmmmST"
two digits "nn"	"KPnnSTP"

The MF KP, ST, and STP digits are mapped as follows:

- * for KP
- # for ST
- B for STP

For example, if ANI and PANI are received, the SIP INVITE contains the following From header:

```
From: <sip:*nnnnnnnnnnnn#*mmmmmmmmmm#@10.2.3.4>;tag=1c14
```



Note: It is possible to remove the * and # characters, using the device's number manipulation rules.

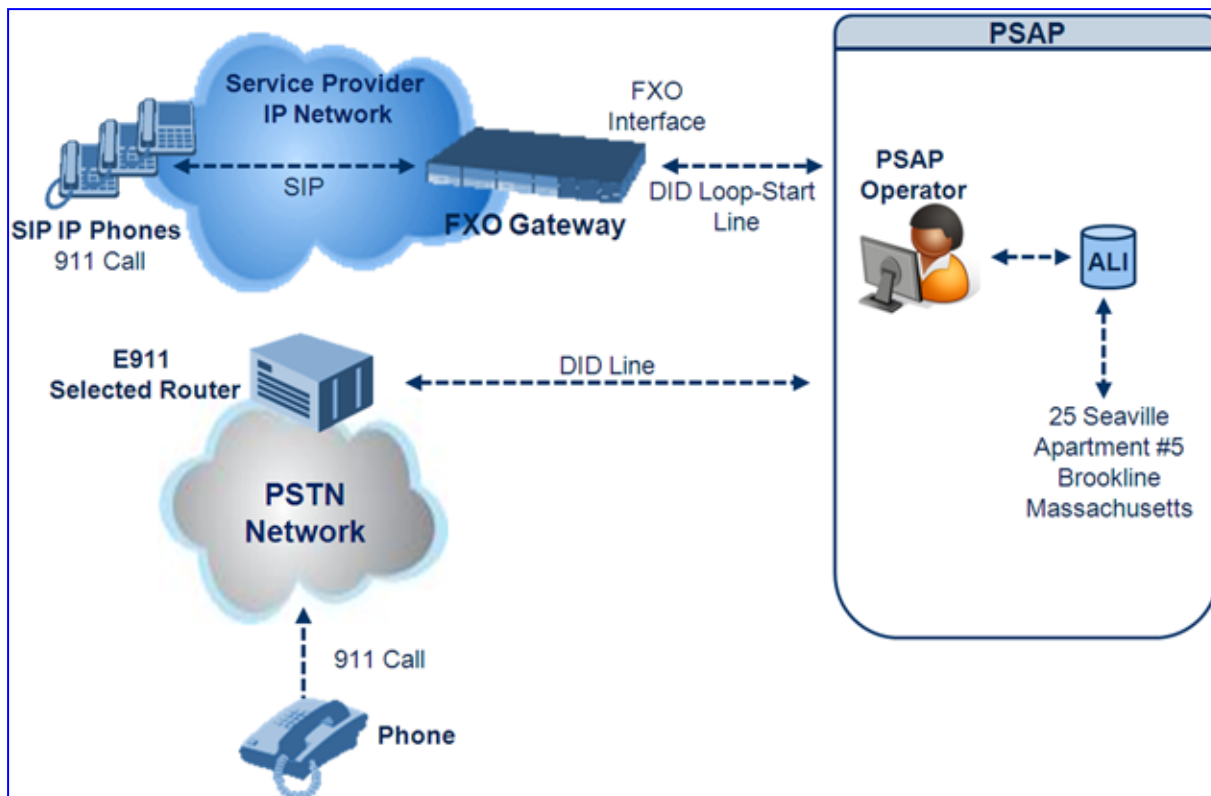
If the device receives the SIP INFO message below, it then generates a "hookflash" mid-call Wink signal:

```
INFO sip:4505656002@192.168.13.40:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.13.2:5060
From: portlvegal <sip:06@192.168.13.2:5060>
To: <sip:4505656002@192.168.13.40:5060>;tag=132878796-1040067870294
Call-ID: 0010-0016-D69A7DA8-1@192.168.13.2
CSeq:2 INFO
Content-Type: application/broadsoft
Content-Length: 17
event flashhook
```

18.5.2.10.2 FXO Device Interworking SIP E911 Calls from Service Provider's IP Network to PSAP DID Lines

The FXO device can interwork SIP emergency E911 calls from the Service Provider's IP network to the analog PSAP DID lines. The standards that define this interface include TR-TSY-000350 or Bellcore's GR-350-Jun2003. This protocol defines signaling between the E911 tandem switch (E911 Selective Router) and the PSAP, using analog loop-start lines. The FXO device can be implemented instead of an E911 switch, by connecting directly to the PSAP DID loop-start lines.

Figure 18-17: FXO Device Interfacing between E911 Switch and PSAP



When an IP phone subscriber dials 911, the device receives the SIP INVITE message and makes a call to the PSAP as follows:

1. The FXO device seizes the line.
2. PSAP sends a Wink signal (250 msec) to the device.
3. Upon receipt of the Wink signal, the device dials MF digits after a user-defined time (WaitForDialTime) containing the caller's ID (ANI) obtained from the SIP headers From or P-Asserted-Identity.
4. When the PSAP operator answers the call, the PSAP sends a polarity reversal to the device, and the device then sends a SIP 200 OK to the IP side.
5. After the PSAP operator disconnects the call, the PSAP reverses the polarity of the line, causing the device to send a SIP BYE to the IP side.
6. If, during active call state, the device receives a Wink signal (typically of 500 msec) from the PSAP, the device generates a SIP INFO message that includes a "hookflash" body, or sends RFC 2833 hookflash Telephony event (according to the HookFlashOption parameter).
7. Following the "hookflash" Wink signal, the PSAP sends DTMF digits. These digits are detected by the device and forwarded to the IP, using RFC 2833 telephony events (or inband, depending on the device's configuration). Typically, this Wink signal followed

by the DTMF digits initiates a call transfer.

For supporting the E911 service, used the following configuration parameter settings:

- Enable911PSAP = 1 (also forces the EnableDIDWink and EnableReversalPolarity)
- HookFlashOption = 1 (generates the SIP INFO hookflash message) or 4 for RFC 2833 telephony event
- WinkTime = 700 (defines detection window of 50 to 750 msec for detection of both winks - 250 msec wink sent by the PSAP for starting the device's dialing; 500 msec wink during the call)
- IsTwoStageDial = 0
- EnableHold = 0
- EnableTransfer = 0
 - Use RFC 2833 DTMF relay:
 - ◆ RxDTMFOption = 3
 - ◆ TxDTMFOption = 4
 - ◆ RFC2833PayloadType = 101
- TimeToSampleAnalogLineVoltage = 100
- WaitForDialTime = 1000 (default is 1 sec)

The device expects to receive the ANI number in the From and/or P-Asserted-Identity SIP header. If the pseudo-ANI number exists, it should be sent as the display name in these headers.

Table 18-16: Dialed Number by Device Depending on Calling Number

Digits of Calling Number (ANI)	Digits of Displayed Number	Number Dialed MF Digits
8 "nnnnnnnn"	-	MF dialed "KPnnnnnnnnST"
12 "nnnnnnnnnnnn"	None	"KPnnnnnnnnnnnnSTP"
12 "nnnnnnnnnnnn"	10 "mmmmmmmmmm" (pANI)	"KPnnnnnnnnnnnnSTKPmmmmmmmmmmST"
2 "nn"	None	"KPnnSTP"
1 "n"	-	MF dialed "KPnST" For example: "From: <sip:8>@xyz.com>" generates device MF spill of KP 8 ST

Table notes:

- For all other cases, a SIP 484 response is sent.
- KP is for .
- ST is for #.
- STP is for B.

The MF duration of all digits, except for the KP digit is 60 msec. The MF duration of the KP digit is 120 msec. The gap duration is 60 msec between any two MF digits.

**Notes:**

- Manipulation rules can be configured for the calling (ANI) and called number (but not on the "display" string), for example, to strip 00 from the ANI "00INXXXXYYY".
- The called number, received as userpart of the Request URI ("301" in the example below), can be used to route incoming SIP calls to FXO specific ports, using the TrunkGroup and PSTNPrefix parameters.
- When the PSAP party off-hooks and then immediately on-hooks (i.e., the device detects wink), the device releases the call sending SIP response "403 Forbidden" and the release reason 21 (i.e., call rejected) "Reason: Q.850 ;cause=21" is sent. Using the cause mapping parameter, it is possible to change the 403 to any other SIP reason, for example, to 603.
- Sometimes a wink signal sent immediately after the FXO device seizes the line is not detected. To overcome this problem, configure the parameter TimeToSampleAnalogLineVoltage to 100 (instead of 1000 msec, which is the default value). The wink is then detected only after this timeout + 50 msec (minimum 150 msec).

Below are two examples for a) INVITE messages and b) INFO messages generated by hook-flash.

- Example (a): INVITE message with ANI = 333333444444 and pseudo-ANI = 0123456789:

```

INVITE sip:301@10.33.37.79;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac771627168
Max-Forwards: 70
From: "0123456789"
<sip:333333444444@audiocodes.com>;tag=1c771623824
To: <sip:301@10.33.37.79;user=phone>
Call-ID: 77162335841200014153@10.33.37.78
CSeq: 1 INVITE
Contact: <sip:101@10.33.37.78>
Supported: em,100rel,timer,replaces,path
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-FXO/v.6.00A.020.077
Privacy: none
P-Asserted-Identity: "0123456789" <sip:333333444444@audiocodes.com>
Content-Type: application/sdp
Content-Length: 253

v=0
o=AudiocodesGW 771609035 771608915 IN IP4 10.33.37.78
s=Phone-Call
c=IN IP4 10.33.37.78
t=0 0
m=audio 4000 RTP/AVP 8 0 101
a=rtpmap:8 pcma/8000
a=rtpmap:0 pcmu/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv

```

- Example (b): The detection of a Wink signal generates the following SIP INFO message:

```
INFO sip:4505656002@192.168.13.40:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.13.2:5060
From: portlvegal <sip:06@192.168.13.2:5060>
To: <sip:4505656002@192.168.13.40:5060>;tag=132878796-1040067870294
Call-ID: 0010-0016-D69A7DA8-1@192.168.13.2
CSeq:2 INFO
Content-Type: application/broadsoft
Content-Length: 17
event flashhook
```

18.5.2.10.3 Pre-empting Existing Calls for E911 IP-to-Tel Calls

If the device receives an E911 call from the IP network destined to the Tel, and there are unavailable channels (e.g., all busy), the device terminates one of the calls (arbitrary) and then sends the E911 call to that channel. The preemption is done only on a channel pertaining to the same Trunk Group for which the E911 call was initially destined and if the channel select mode (configured by the ChannelSelectMode parameter) is set to other than “By Dest Number” (0).

The preemption is done only if the incoming IP-to-Tel call is identified as an emergency call. The device identifies emergency calls by one of the following:

- The destination number of the IP call matches one of the numbers defined by the EmergencyNumbers parameter. (For E911, you must defined this parameter with the value "911".)
- The incoming SIP INVITE message contains the “emergency” value in the Priority header.

This feature is enabled by setting the CallPriorityMode parameter to “Emergency” (2).



Notes:

- This feature is applicable to FXO, CAS, and ISDN interfaces.
- For FXO interfaces, the preemption is done only on existing IP-to-Tel calls. In other words, if all the current FXO channels are busy with calls that were answered by the FXO device (i.e., Tel-to-IP calls), new incoming emergency IP-to-Tel calls are rejected.

18.5.2.11 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 one of those listed in the table below. A default MLPP call Precedence Level (configured by the SIPDefaultCallPriority parameter) is used if the incoming SIP INVITE or PRI Setup message contains an invalid priority or Precedence Level value respectively. For each MLPP call priority level, the Multiple Differentiated Services Code Points (DSCP) can be set to a value from 0 to 63.

Table 18-17: 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	MLPPIImmediateRTPDSCP
6	flash	MLPPFlashRTPDSCP
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. In addition, you can define (using the PreemptionToneDuration parameter) the duration for which the device plays a preemption tone to the Tel and IP sides if a call is preempted.
 - 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 include one of the following preemption cause classes:
 - Reason: preemption ;cause=1 ;text="UA Preemption"
 - Reason: preemption ;cause=2 ;text="Reserved Resources Preempted"
 - Reason: preemption ;cause=3 ;text="Generic Preemption"
 - Reason: preemption ;cause=4 ;text="Non-IP Preemption"
 - 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



Notes:

- If required, you can exclude the "resource-priority" tag from the SIP Require header in INVITE messages for Tel-to-IP calls when MLPP priority call handling is used. This is configured using the RPRRequired parameter.
- For a complete list of the MLPP parameters, see 'MLPP Parameters' on page 664.

18.5.2.12 Denial of Collect Calls

You can configure the device to reject (disconnect) incoming Tel-to-IP collect calls and to signal this denial to the PSTN. This capability is required, for example, in the Brazilian telecommunication system to deny collect calls. When this feature is enabled upon rejecting the incoming call, the device sends a sequence of signals to the PSTN. This consists of an off-hook, an on-hook after one second, and then an off-hook after two seconds. In other words, this is in effect, a double-answer sequence.

This feature is enabled for all calls, using the EnableFXODoubleAnswer parameter.

**Notes:**

- This feature is applicable only to FXO interfaces.
- To support this feature, ensure that automatic dialing has not been configured for the FXO ports.
- Ensure that the PSTN side is configured to identify this double-answer signal.

18.5.3 Configuring ISDN Supplementary Services

The ISDN Supp Services Table page allows you to configure supplementary services for Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI) phones connected to the device. This feature enables the device to route IP-to-Tel calls (including voice and fax) to specific BRI ports (channels).

This table allows you to define BRI phone extension numbers per BRI port pertaining to a specific BRI module. Therefore, this offers support for point-to-multipoint configuration of several phone numbers per BRI channel. Up to eight phone numbers can be defined per BRI trunk. In addition, for each BRI endpoint, the following optional configurations can be defined:

- User ID and password - for registering the BRI endpoint to a third-party softswitch for authentication and/or billing. For viewing BRI registration status, see 'Viewing Registration Status' on page 509.
- Caller ID name - for displaying the BRI endpoint's caller ID to a dialed destination, if enabled (i.e., "Presentation" is not restricted)
- Caller ID presentation or restriction
- Enable/disable sending caller ID to BRI endpoints

**Notes:**

- To use this table for routing of IP-to-Tel calls to specific BRI channels, the Channel Select Mode in the Trunk Group Settings must be set to 'Select Trunk by ISDN Supplementary Services Table' (see 'Configuring Trunk Group Settings' on page 251).
- You can also configure this table using the ISDNSuppServ *ini* file table parameter (see 'Configuration Parameters Reference' on page 529).
- To allow the end-user to hear a dial tone when picking up the BRI phone, it is recommended to set the Progress Indicator in the Setup Ack bit (0x10000=65536). Therefore, the recommended value is 0x10000 + 0x1000 = 65536 + 4096 = 69632 (i.e., set the ISDNInCallsBehavior parameter to 69632).

➤ **To configure BRI supplementary services:**

1. Open the ISDN Supp Services Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Digital Gateway** submenu > **ISDN Supp Services**).

Figure 18-18: ISDN Supp Services Table Page

Index	Phone Number	Module	Port	User ID
1 <input type="radio"/>	4112	1	3	mike
2 <input type="radio"/>		0	0	

↓

User Password	Caller ID	Presentation Restricted	Caller ID Enabled
*	mike	Allowed	Enabled
*		Not Configured	Not Configured

2. Configure the parameters as described in the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.
5. To register the BRI endpoints, click the **Register** button. To unregister the BRI endpoints, click **Unregister**. The registration method for each BRI endpoint is according to the setting of the 'Registration Mode' parameter in the Trunk Group Settings page.

Table 18-18: ISDN Supp Services Table Parameters

Parameter	Description
Phone Number	The telephone extension number for the BRI endpoint.
Module	The BRI module number to which the BRI extension pertains.
Port	The port number (on the BRI module) to which the BRI extension is connected.
User ID	User ID for registering the BRI endpoint to a third-party softswitch for authentication and/or billing.
User Password	User password for registering the BRI endpoint to a third-party softswitch for authentication and/or billing. Note: For security, the password is displayed as an asterisk (*).
Caller ID	Caller ID name of the BRI extension (sent to the IP side). The valid value is a string of up to 18 characters.
Presentation Restricted	Determines whether the BRI extension sends its Caller ID information to the IP when a call is made. <ul style="list-style-type: none"> ▪ [0] Allowed = The device sends the string defined in the 'Caller ID' field when this BRI extension makes a Tel-to-IP call. ▪ [1] Restricted = The string defined in the 'Caller ID' field is not sent.
Caller ID Enabled	Enables the receipt of Caller ID. <ul style="list-style-type: none"> ▪ [0] Disabled = The device does not send Caller ID information to the BRI extension. ▪ [1] Enabled = The device sends Caller ID information to the BRI extension

18.5.4 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 529.



Notes:

- The Voice Mail Settings page is available only for FXO and CAS interfaces.
- For more information on configuring voice mail, refer to the *CPE Configuration Guide for Voice Mail User's Manual*.

➤ To configure the Voice Mail parameters:

1. Open the Voice Mail Settings page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Advanced Applications** submenu > **Voice Mail Settings**).

Line Transfer Mode	None	▼
Voice Mail Interface	NONE	▼
▼ Digit Patterns		
Forward on Busy Digit Pattern (Internal)	<input type="text"/>	
Forward on No Answer Digit Pattern (Internal)	<input type="text"/>	
Forward on Do Not Disturb Digit Pattern (Internal)	<input type="text"/>	
Forward on No Reason Digit Pattern (Internal)	<input type="text"/>	
Forward on Busy Digit Pattern (External)	<input type="text"/>	
Forward on No Answer Digit Pattern (External)	<input type="text"/>	
Forward on Do Not Disturb Digit Pattern (External)	<input type="text"/>	
Forward on No Reason Digit Pattern (External)	<input type="text"/>	
Internal Call Digit Pattern	<input type="text"/>	
External Call Digit Pattern	<input type="text"/>	
Disconnect Call Digit Pattern	<input type="text"/>	
Digit To Ignore Digit Pattern	<input type="text"/>	
▼ Message Waiting Indication (MWI)		
MWI Off Digit Pattern	<input type="text"/>	
MWI On Digit Pattern	<input type="text"/>	
MWI Suffix Pattern	<input type="text"/>	
MWI Source Number	<input type="text"/>	
▼ SMDI		
⚡ Enable SMDI	Disable	▼
SMDI Timeout [msec]	2000	

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

18.5.5 Advice of Charge Services for Euro ISDN

Advice of charge (AOC) is a pre-billing function that tasks the rating engine with calculating the cost of using a service and relaying that information back to the customer thus, allowing users to obtain charging information for all calls during the call (AOC-D) or at the end of the call (AOC-E), or both.

The AOC-D and AOC-E messages are part of the Facility Information Element (IE) message:

- AOC-D message—ISDN Advice of Charge information sent during a call. The message is sent periodically to subscribers of AOC during-call services.
- AOC-E message—ISDN Advice of Charge information sent at the end of a call.

The device supports the sending of AoC messages for Tel-to-IP calls, providing billing applications with the number of charged units. This feature can typically be implemented in the hotel industry, where external calls made by guests can be billed accurately. In such a setup, the device is connected on one side to a PBX through an E1 line (Euro ISDN), and on the other side to a SIP trunk provided by an ITSP. When a call is made by a guest, the device first sends an AOC-D Facility message to the PBX indicating the connection charge unit, and then sends subsequent AOC-D messages every user-defined interval to indicate the charge unit during the call. When the call ends, the device sends an AoC-E Facility message to the PBX indicating the total number of charged units.

To configure AoC:

1. Ensure that the PSTN protocol for the E1 trunk line is Euro ISDN and set to network side.
2. Ensure that the date and time of the device is correct. For accuracy, it is recommended to use an NTP server to obtain the date and time.
3. Enable the AoC service, using the EnableAOC parameter.
4. Configure charge codes in the Charge Code table (ChargeCode) - see Configuring Charge Codes on page 314. Note that in the Charge Code table, the table fields are as follows:
 - 'End Time' - time at which this charge code ends
 - 'Pulse Interval' - time between every sent AOC-D Facility message
 - 'Pulses On Answer' - number of charging units in first generated AOC-D Facility message
5. Assign the charge code index to the desired routing rule in the Outbound IP Routing table (see 'Configuring Outbound IP Routing Table' on page 269).

18.6 Analog Gateway

This section describes configuration of analog settings.



Note: The Analog Gateway submenu appears only if the device is installed with an FXS or FXO module.

18.6.1 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 [319](#)
- Caller ID Restriction - see 'Configuring Caller Display Information' on page [318](#)
- Hotline - see 'Configuring Automatic Dialing' on page [317](#)
- Call Transfer
- Call Waiting - see 'Configuring Call Waiting' on page [321](#)
- 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 18-19: Keypad Features Page

▼ Forward	
Unconditional	<input type="text"/>
No Answer	<input type="text"/>
On Busy	<input type="text"/>
On Busy or No Answer	<input type="text"/>
Do Not Disturb	<input type="text"/>
Deactivate	<input type="text"/>
▼ Caller ID Restriction	
Activate	<input type="text"/>
Deactivate	<input type="text"/>
▼ Hotline	
Activate	<input type="text"/>
Deactivate	<input type="text"/>
▼ Transfer	
Blind	<input type="text"/>
▼ Call Waiting	
Activate	<input type="text"/>
Deactivate	<input type="text"/>
▼ Reject Anonymous Call	
Activate	<input type="text"/>
Deactivate	<input type="text"/>

2. Configure the keypad features as required. For a description of these parameters, see 'Configuration Parameters Reference' on page 529.
3. Click **Submit** to apply your changes.
4. To save the changes to the flash memory, see 'Saving Configuration' on page 470.

18.6.2 Configuring Metering Tones

The FXS interfaces can generate 12/16 KHz metering pulses toward the Tel side (e.g., for connection to a pay phone or private meter). Tariff pulse rate is determined according to the device's Charge Codes table. This capability enables users to define different tariffs according to the source/destination numbers and the time-of-day. The tariff rate includes the time interval between the generated pulses and the number of pulses generated on answer.


**Notes:**

- The Metering Tones page is available only for FXS interfaces.
- Charge Code rules can be assigned to routing rules in the 'Outbound IP Routing Table' (see 'Configuring Outbound IP Routing Table' on page 269). When a new call is established, the 'Outbound IP Routing Table' is searched for the destination IP address. Once a route is located, the Charge Code (configured for that route) is used to associate the route with an entry in the Charge Codes table.


➤ **To configure Metering tones:**

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

Figure 18-20: Metering Tones Page

Generate Metering Tones	Disable	▼
⚡ Metering Tone Type	16 KHz	▼
Charge Codes Table		

2. Configure the Metering tones parameters as required. For a description of the parameters appearing on this page, see 'Configuration Parameters Reference' on page 529.
3. Click **Submit** to apply your changes.
4. To save the changes to the flash memory, see 'Saving Configuration' on page 470.

If you set the 'Generate Metering Tones' parameter to **Internal Table**, access the Charge Codes Table page by clicking the **Charge Codes Table**  button. For more information on configuring the Charge Codes table, see 'Configuring Charge Codes Table' on page 314.

18.6.3 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 Outbound IP Routing Table'.



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.
- The Charge Codes table can also be used to configure Advice of Charge (AoC) services for Euro ISDN trunks (see Advice of Charge Services for Euro ISDN on page 310).

➤ **To configure the Charge Codes:**

1. Open the Charge Codes Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Charge Codes**). Alternatively, you can access this page from the Metering Tones page (see 'Configuring Metering Tones' on page 312).

Figure 18-21: Charge Codes Table Page

Table Index												
												0-4
Index	Time Period 1			Time Period 2			Time Period 3			Time Period 4		
	End Time	Pulse Interval	Pulses On Answer	End Time	Pulse Interval	Pulses On Answer	End Time	Pulse Interval	Pulses On Answer	End Time	Pulse Interval	Pulses On Answer
0	07	30	1	14	20	2	20	15	1	00	60	1
1	05	60	1	14	20	1	00	60	1			
2	00	60	1									
3												
4												

2. 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 **Submit** to apply your changes.
4. To save the changes to the flash memory, see 'Saving Configuration' on page 470.

18.6.4 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 529.



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 18-22: FXO Settings Page

Dialing Mode	Two Stages	▼
Waiting for Dial Tone	No	▼
Time to Wait before Dialing [msec]	1000	
Ring Detection Timeout [sec]	8	
Reorder Tone Duration [sec]	255	
Answer Supervision	No	▼
Rings before Detecting Caller ID	1	▼
Send Metering Message to IP	No	▼
Disconnect Call on Busy Tone Detection (CAS)	Enable	▼
Disconnect On Dial Tone	Disable	▼
Guard Time Between Calls	1	
FXO AutoDial Play BusyTone	Disable	▼

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

18.6.5 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 **Submit**, the password is displayed as an asterisk (*).
- You can also configure Authentication using the *ini* file table parameter Authentication (see 'Configuration Parameters Reference' on page 529).

➤ **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**).

Figure 18-23: Authentication Page

Gateway Port	User Name	Password
Module 1 Port 1 FXS	<input type="text" value="user1"/>	<input type="password" value="* * * * *"/>
Module 1 Port 2 FXS	<input type="text" value="user2"/>	<input type="password" value="* * * * *"/>
Module 2 Port 1 FXO	<input type="text"/>	<input type="password"/>
Module 2 Port 2 FXO	<input type="text"/>	<input type="password"/>
Module 2 Port 3 FXO	<input type="text"/>	<input type="password"/>
Module 2 Port 4 FXO	<input type="text"/>	<input type="password"/>

3. In the 'User Name' and 'Password' fields corresponding to a port, enter the user name and password respectively.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 470.

18.6.6 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 'Configuration Parameters Reference' on page 529).

➤ 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**).

Gateway Port	Destination Phone Number	Auto Dial Status
Module 1 Port 1 FXS	<input type="text" value="101"/>	Enable <input type="button" value="v"/>
Module 1 Port 2 FXS	<input type="text" value="911"/>	Hotline <input type="button" value="v"/>
Module 2 Port 1 FXO	<input type="text" value="302"/>	Enable <input type="button" value="v"/>
Module 2 Port 2 FXO	<input type="text"/>	Enable <input type="button" value="v"/>
Module 2 Port 3 FXO	<input type="text"/>	Enable <input type="button" value="v"/>
Module 2 Port 4 FXO	<input type="text"/>	Enable <input type="button" value="v"/>

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 **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 470.

18.6.7 Configuring Caller Display Information

The Caller Display Information page [allows](#) you to define a caller identification string (Caller ID) for FXS and FXO ports and enable the device to send the 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 254.

➤ **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**).

Gateway Port	Caller ID/Name	Presentation
Module 1 Port 1 FXS	Private	Restricted ▼
Module 1 Port 2 FXS	Susan C.	Restricted ▼
Module 2 Port 1 FXO	Lee P.	Allowed ▼
Module 2 Port 2 FXO	Ronaldo	Allowed ▼
Module 2 Port 3 FXO		Allowed ▼
Module 2 Port 4 FXO		Allowed ▼

2. 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 **Submit** to apply your changes.
5. To save the changes to flash memory, see 'Saving Configuration' on page 470.

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).
- 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 254).
- You can also configure the Caller Display Information table using the *ini* file table parameter CallerDisplayInfo.



18.6.8 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 283).
- 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**).

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

2. Configure the Call Forward parameters for each port according to the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

Table 18-19: Call Forward Table

Parameter	Description
Forward Type	<p>Determines the scenario for forwarding a call.</p> <ul style="list-style-type: none"> ▪ [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	<p>The telephone number or URI (<number>@<IP address>) to where the call is forwarded.</p> <p>Note: If this field only contains a telephone number and a Proxy isn't</p>

Parameter	Description
	used, the 'forward to' phone number must be specified in the Outbound IP Routing Table' (see 'Configuring Outbound IP Routing Table' on page 269).
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.

18.6.9 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 283.



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**).

Gateway Port	Caller ID
Module 1 Port 1 FXS	Enable ▾
Module 1 Port 2 FXS	Disable ▾
Module 2 Port 1 FXO	▾
Module 2 Port 2 FXO	▾
Module 2 Port 3 FXO	▾
Module 2 Port 4 FXO	▾

2. 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 283).
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

18.6.10 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 283).
- You can also configure the Call Waiting table using the *ini* file table parameter CallWaitingPerPort (see 'Configuration Parameters Reference' on page 529).
- 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 Call Waiting page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Analog Gateway** submenu > **Call Waiting**).

Gateway Port	Call Waiting Configuration
Module 1 Port 1 FXS	Enable ▼
Module 1 Port 2 FXS	Enable ▼
Module 2 Port 1 FXO	▼
Module 2 Port 2 FXO	▼
Module 2 Port 3 FXO	▼
Module 2 Port 4 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 283).
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

18.6.11 Configuring FXS Distinctive Ringing and Call Waiting Tones per Source/Destination Number

You can configure a Distinctive Ringing tone and Call Waiting tone per calling (source) and/or called (destination) number (or prefix) for IP-to-Tel calls. This feature can be configured per FXS endpoint or for a range of FXS endpoints. Therefore, different tones can be played per FXS endpoint/s depending on the source and/or destination number of the received call. In addition, you can configure multiple entries with different source and/or destination prefixes and tones for the same FXS port.

Typically, the played Ringing and/or Call Waiting tone is indicated in the SIP Alert-info header field of the received INVITE message. If this header is not present in the received INVITE, then this feature is used and the tone played is according to the settings in this table.



Notes:

- This page is applicable only to FXS interfaces.
- You can also configure the Tone Index table using the *ini* file table parameter ToneIndex.

➤ **To configure distinctive ringing and call waiting per FXS port:**

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

Figure 18-24: Tone Index Table Page

Index	FXS Port First	FXS Port Last	Source Prefix	Destination Prefix	Priority Index
1	1	4	2		1

The figure above shows a configuration example for using 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.

2. In the 'Add' field, enter a table index number and then click **Add**.
3. Configure the table according to the table below.
4. Click **Submit** to apply your changes.

Table 18-20: Tone index Table Parameter Description

Parameter	Description
Index	Defines the table index entry. Up to 50 entries can be defined.
FXS Port First	Defines the starting range of FXS ports, where 1 is the first port.
FXS Port Last	Defines the end range of FXS ports.
Source Prefix	Defines the prefix of the calling number.
Destination Prefix	Defines the prefix of the called number.
Priority Index	Defines the index of the Distinctive Ringing and Call Waiting tones (default is 0). The Call Waiting tone index equals to the Priority Index plus the value of the FirstCallWaitingToneID parameter. For example, if you want to use the Call Waiting tone in the CPT file at Index #9, you need to enter "1" as the Priority Index value and set the FirstCallWaitingToneID parameter to "8". The summation of these values is 9, i.e., index #9.

18.6.12 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 166).

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

18.6.13 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 323)
- For Tel-to-IP calls (see 'FXO Operations for Tel-to-IP Calls' on page 326)
- Call termination on FXO devices (see 'Call Termination on FXO Devices' on page 328)

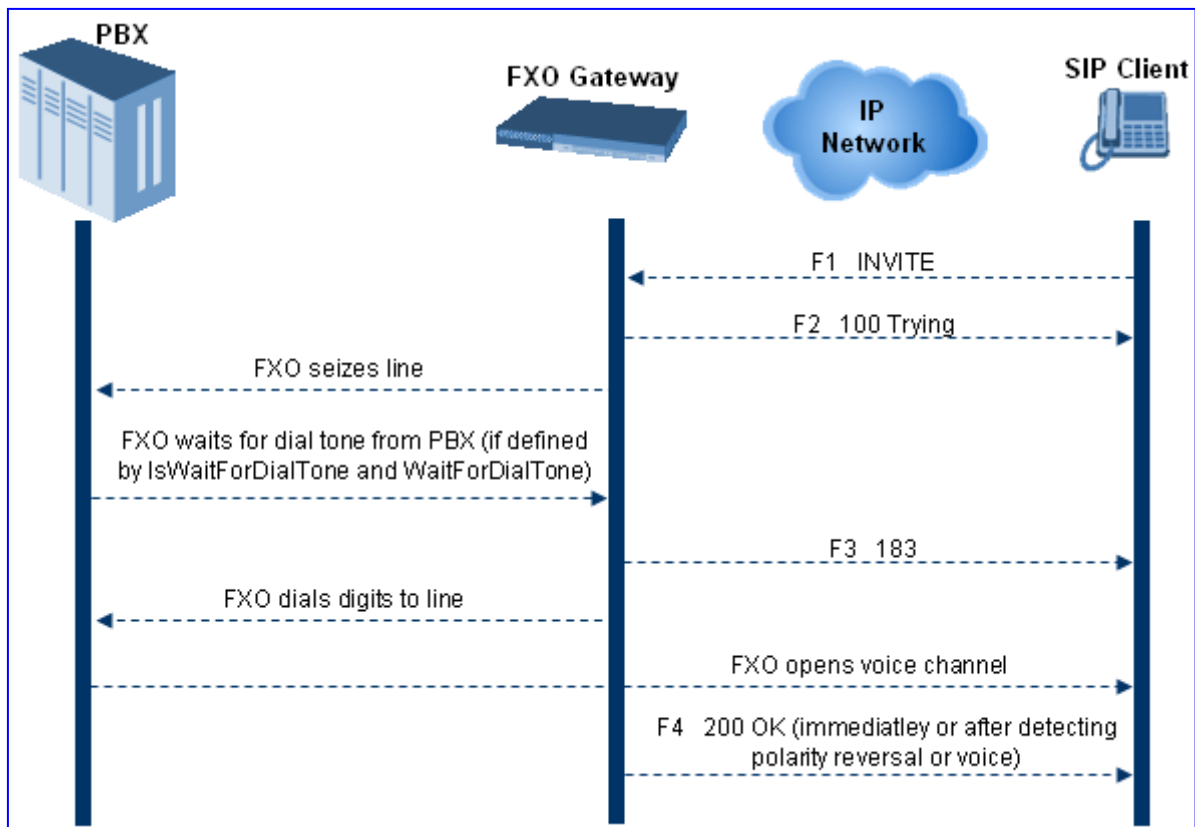
18.6.13.1 FXO Operations for IP-to-Tel Calls

The FXO device provides the following operating modes for IP-to-Tel calls:

- One-stage dialing (see 'One-Stage Dialing' on page 324)
 - Waiting for dial tone (see 'Two-Stage Dialing' on page 325)
 - Time to wait before dialing
 - Answer supervision
- Two-stage dialing (see 'Two-Stage Dialing' on page 325)
- Dialing time: DID wink (see 'DID Wink' on page 325)

18.6.13.1.1 One-Stage Dialing

One-stage dialing is when the FXO device receives an IP-to-Tel call, off-hooks the PBX line connected to the telephone, and then immediately dials the destination telephone number. In other words, the IP caller doesn't dial the PSTN number upon hearing a dial tone.



One-stage dialing incorporates the following FXO functionality:

- **Waiting for Dial Tone:** Enables the device to dial the digits to the Tel side only after detecting a dial tone from the PBX line. The *ini* file parameter `IsWaitForDialTone` is used to configure this operation.
- **Time to Wait Before Dialing:** Defines the time (in msec) between seizing the FXO line and starting to dial the digits. The *ini* file parameter `WaitForDialTime` is used to configure this operation.



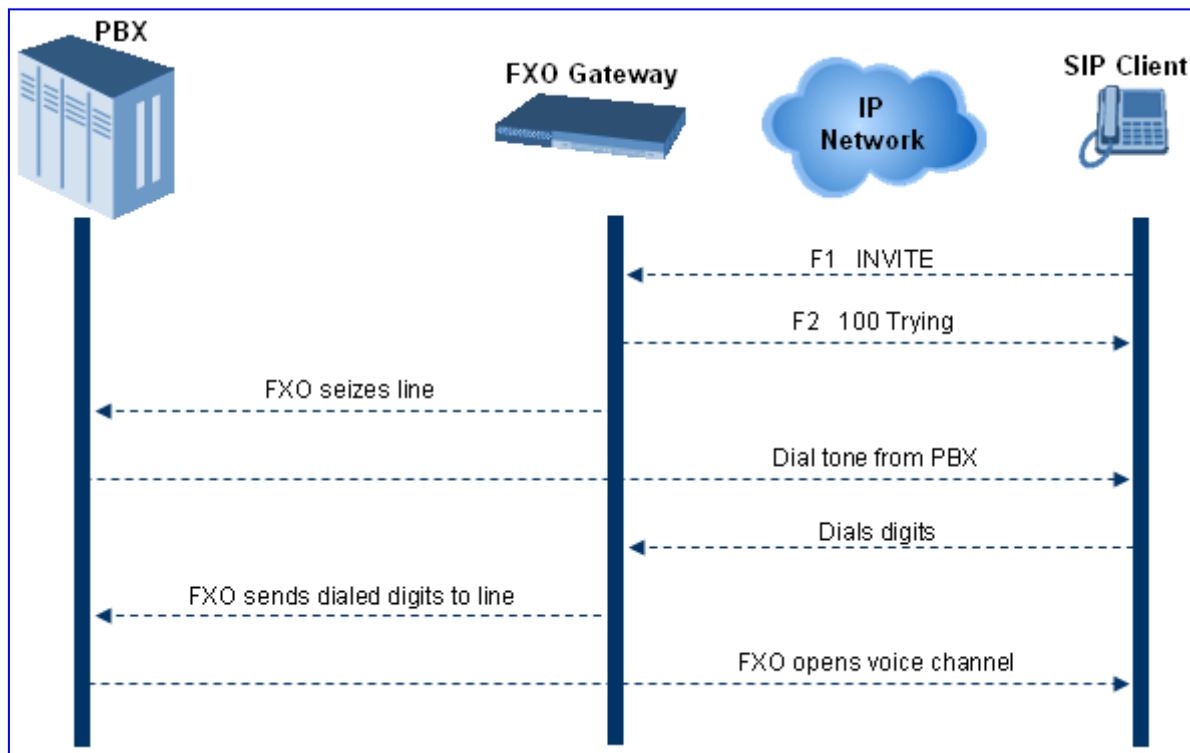
Note: The *ini* file parameter `IsWaitForDialTone` must be disabled for this mode.

- **Answer Supervision:** The Answer Supervision feature enables the FXO device to determine when a call is connected, by using one of the following methods:
 - **Polarity Reversal:** the device sends a 200 OK in response to an INVITE only when it detects a polarity reversal.
 - **Voice Detection:** the device sends a 200 OK in response to an INVITE only when it detects the start of speech (or ringback tone) from the Tel side. (Note that the IPM detectors must be enabled).

18.6.13.1.2 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 18-25: 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

18.6.13.1.3 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

18.6.13.2 FXO Operations for Tel-to-IP Calls

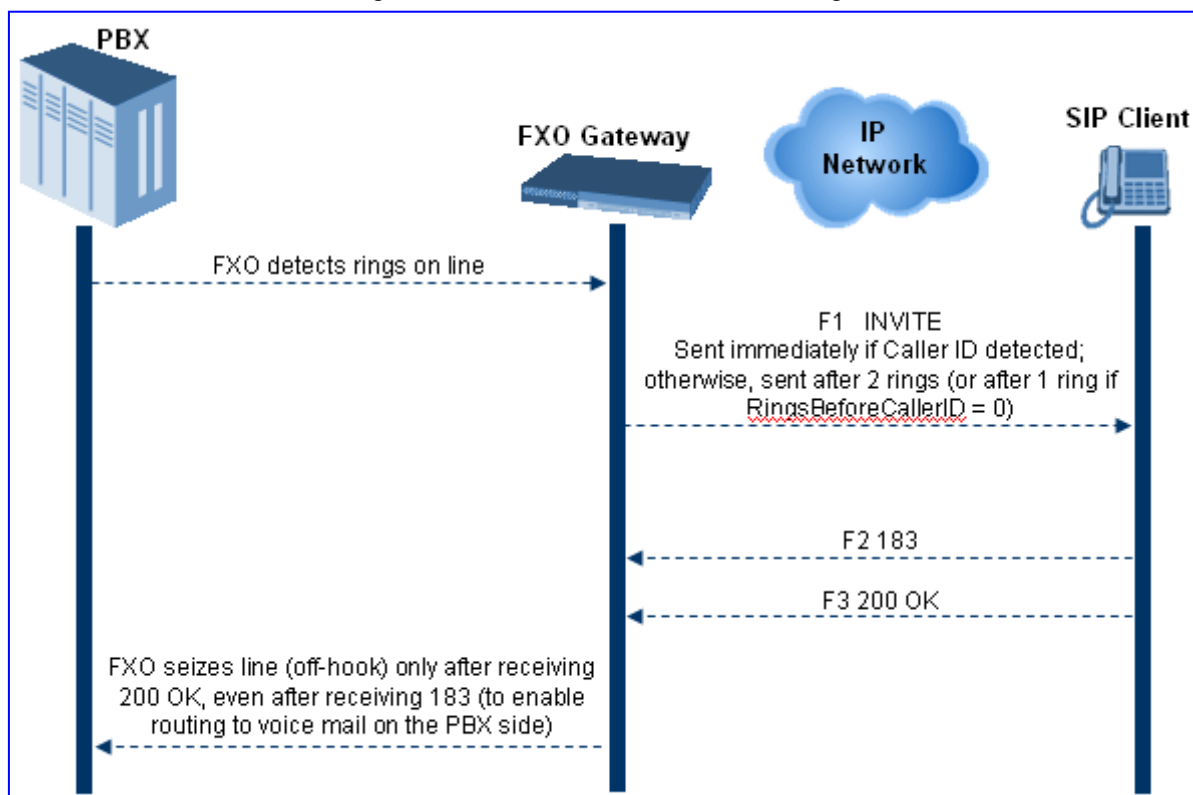
The FXO device provides the following FXO operating modes for Tel-to-IP calls:

- Automatic Dialing (see 'Automatic Dialing' on page 326)
- Collecting Digits Mode (see 'Collecting Digits Mode' on page 327)
- FXO Supplementary Services (see 'FXO Supplementary Services' on page 327)
 - Hold/Transfer Toward the Tel side
 - Hold/Transfer Toward the IP side
 - Blind Transfer to the Tel side

18.6.13.2.1 Automatic Dialing

Automatic dialing is defined using the Web interface's Automatic Dialing (TargetOfChannel ini file parameter) page, described in see 'Configuring Automatic Dialing' on page 317.

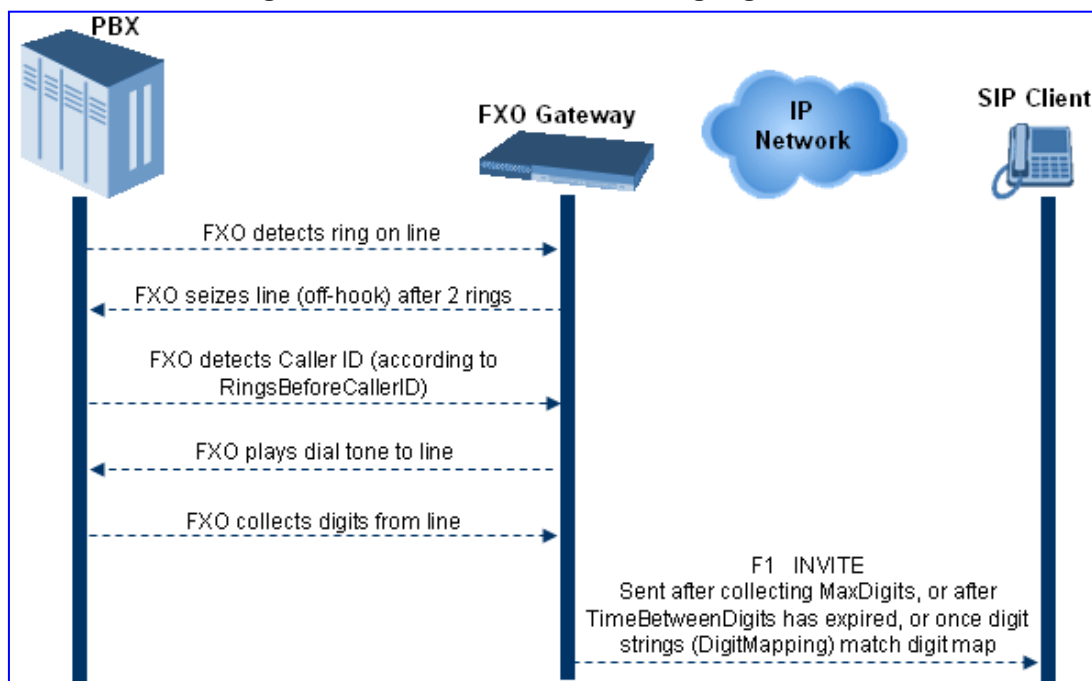
The SIP call flow diagram below illustrates Automatic Dialing.



18.6.13.2.2 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 18-26: Call Flow for Collecting Digits Mode



18.6.13.2.3 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.

18.6.13.3 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 328)
- Calls terminated before call establishment (see 'Call Termination before Call Establishment' on page 329)
- Ring detection timeout (see 'Ring Detection Timeout' on page 329)

18.6.13.3.1 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.
- **Special DTMF code:** A digit pattern that when received from the Tel side, indicates to the device to disconnect the call.
- **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.

18.6.13.3.2 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.

18.6.13.3.3 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).

18.6.14 Remote PBX Extension Between FXO and FXS Devices

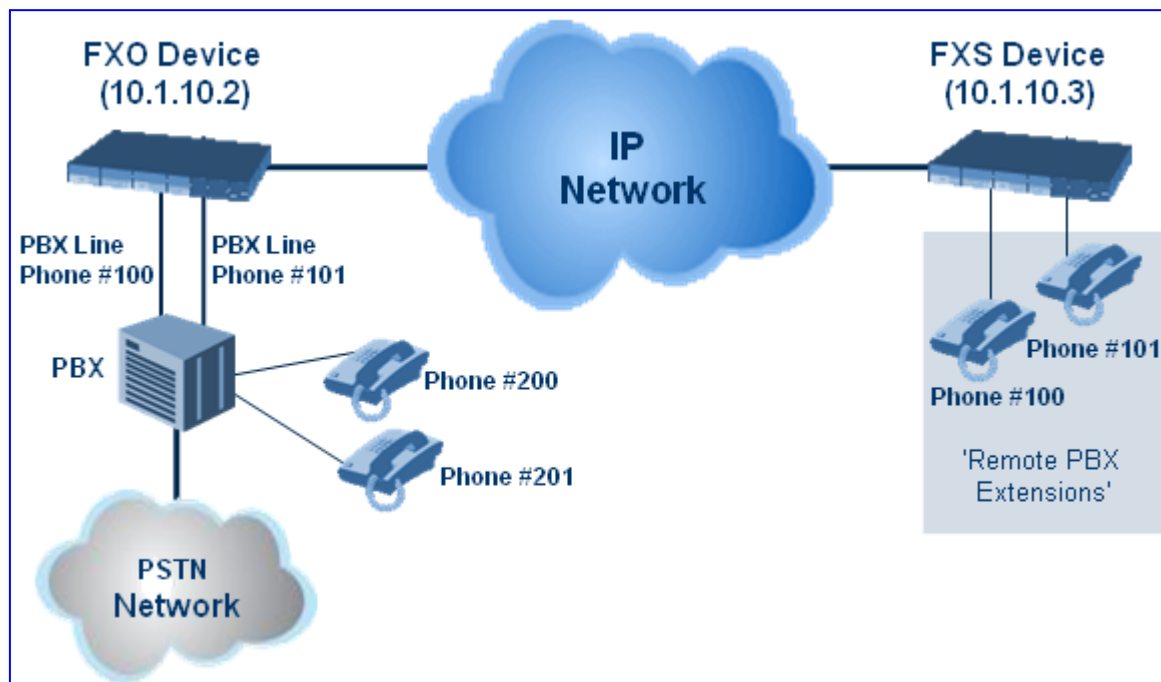
Remote PBX extension offers a company the capability of extending the "power" of its local PBX by allowing remote phones (remote offices) to connect to the company's PBX over the IP network (instead of via PSTN). This is as if the remote office is located in the head office (where the PBX is installed). PBX extensions are connected through FXO ports to the IP network, instead of being connected to individual telephone stations. At the remote office, FXS units connect analog phones to the same IP network. To produce full transparency, each FXO port is mapped to an FXS port (i.e., one-to-one mapping). This allows individual extensions to be extended to remote locations. To call a remote office worker, a PBX user or a PSTN caller simply dials the PBX extension that is mapped to the remote FXS port.

This section provides an example on how to implement a remote telephone extension through the IP network, using FXO and FXS interfaces. In this configuration, the FXO device routes calls received from the PBX to the 'Remote PBX Extension' connected to the FXS device. The routing is transparent as if the telephone connected to the FXS device is directly connected to the PBX.

The following is required:

- FXO interfaces with ports connected directly to the PBX lines (shown in the figure below)
- FXS interfaces for the 'remote PBX extension'

- Analog phones (POTS)
- PBX (one or more PBX loop start lines)
- LAN network



18.6.14.1 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.

18.6.14.2 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.

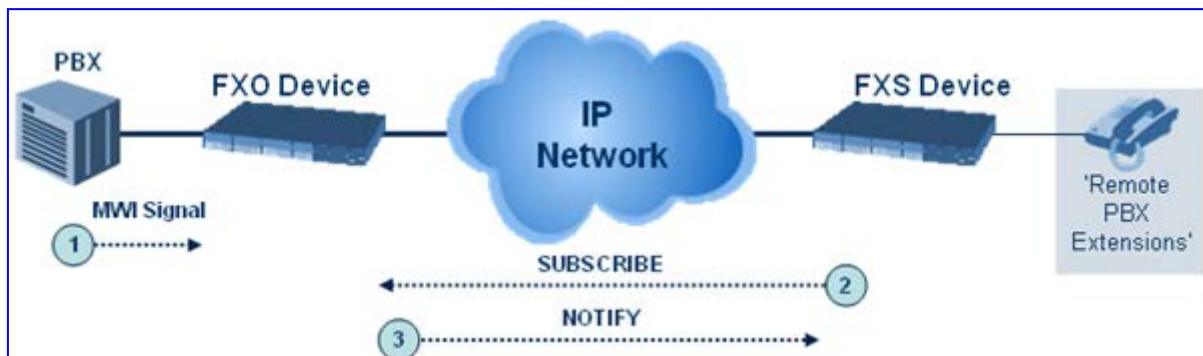
18.6.14.3 Message Waiting Indication for Remote Extensions

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.



18.6.14.4 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.



18.6.14.5 FXS Gateway Configuration

The procedure below describes how to configure the FXS interface (at the 'remote PBX extension').

➤ **To configure the FXS interface:**

1. In the Trunk Group Table page (see Configuring Trunk Group Table on page 249, assign the phone numbers 100 to 104 to the device's endpoints.

Figure 18-27: Assigning Phone Numbers to FXS Endpoints

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID
1	Module 3 FXS	1	1	1-4	100	0

2. In the Automatic Dialing page (see 'Configuring Automatic Dialing' on page 317), 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 18-28: Automatic Dialing for FXS Ports

Gateway Port	Destination Phone Number	Auto Dial Status
Module 3 Port 1 FXS	200	Enable
Module 3 Port 2 FXS	201	Enable
Module 3 Port 3 FXS	202	Enable
Module 3 Port 4 FXS	203	Enable

3. In the Outbound IP Routing Table page (see 'Configuring Outbound IP Routing Table' on page 269), enter 20 for the destination phone prefix, and 10.1.10.2 for the IP address of the FXO device.

Figure 18-29: FXS Tel-to-IP Routing Configuration

	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address
1		20	*	10.1.10.2



Note: For the transfer to function in remote PBX extensions, Hold must be disabled at the FXS device (i.e., Enable Hold = 0) and hook-flash must be transferred from the FXS to the FXO (HookFlashOption = 4).

18.6.14.6 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 Trunk Group Table page (see Configuring Trunk Group Table on page 249, assign the phone numbers 200 to 204 to the device's FXO endpoints.

Figure 18-30: Assigning Phone Numbers to FXO Ports

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number
1	Module 3 FXO ▾			1-4	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 18-31: FXO Automatic Dialing Configuration

Gateway Port	Destination Phone Number	Auto Dial Status
Module 3 Port 1 FXO	100	Enable ▾
Module 3 Port 2 FXO	101	Enable ▾
Module 3 Port 3 FXO	102	Enable ▾
Module 3 Port 4 FXO	103	Enable ▾

3. In the Outbound IP Routing Table page, enter 10 in the 'Destination Phone Prefix' field, and the IP address of the FXS device (10.1.10.3) in the field 'IP Address'.

Figure 18-32: 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 315), set the parameter 'Dialing Mode' to **Two Stages** (IsTwoStageDial = 1).

18.7 Dialing Plan Features

This section discusses various dialing plan features supported by the device:

- Digit mapping (see 'Digit Mapping' on page 334)
- External Dial Plan file containing dial plans (see 'External Dial Plan File' on page 335)
- Dial plan prefix tags for enhanced IP-to-Tel routing (see Dial Plan Prefix Tags for IP-to-Tel Routing on page 338)

18.7.1 Digit Mapping

Digit map pattern rules are used for Tel-to-IP ISDN overlap dialing (by setting the ISDNRxOverlap parameter to 1) to reduce the dialing period (for digital interface). For more information on digit maps for ISDN overlapping, see ISDN Overlap Dialing on page 244. 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 18-21: 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|91xxxxxxxxxxx|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 335), 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.



18.7.2 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 335), 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 being completed in the Dial Plan.
- For E1 CAS MFC-R2 variants (which don't support terminating digit for the called party number, usually I-15), the external Dial Plan file and the DigitMapping parameter are ignored. Instead, you can define a Dial Plan template per trunk using the parameter CasTrunkDialPlanName_x.



18.7.2.1 Modifying ISDN-to-IP Calling Party Number

The device can use the Dial Plan file to change the Calling Party Number value (source number) of the incoming ISDN call when sending to IP. For this feature, the Dial Plan file supports the following syntax:

<ISDN Calling Party Number>,0,<new calling number>

- The first number contains the calling party number (or its prefix) received in the ISDN call SETUP message. The source number can also be a range, using the syntax [x-y] in the Dial Plan file. This number is used as the display name in the From header of the outgoing INVITE.
- The second number must always be set to "0".
- The third number is a string of up to 12 characters containing the mapped number that is used as the URI user part in the From and Contact headers of the outgoing INVITE.

The Dial Plan index used in the Dial Plan file for this feature is defined by the Tel2IPSourceNumberMappingDialPlanIndex parameter.

An example of such a configuration in the Dial Plan file is shown below:

```
[ PLAN1 ]
; specific received number changed to 04343434181.
0567811181,0,04343434181
; number range that changes to 04343434181.
056788118[2-4],0,04343434181
```

If we take the first Dial Plan rule in the example above (i.e., "0567811181,0,04343434181"), the received Calling Number Party of 0567811181 is changed to 04343434181 and sent to the IP with a SIP INVITE as follows:

```
Via: SIP/2.0/UDP 211.192.160.214:5060;branch=z9hG4bK3157667347
From: <sip:04343434181@kt.co.kr:5060>;tag=de0004b1
To: sip:01066557573@kt.co.kr:5060
Call-ID: 585e60ec@211.192.160.214
CSeq: 1 INVITE
Contact:<sip:04343434181@211.192.160.214:5060;transport=udp>
```

The initial Dial Plan text file must be converted to *.dat file format using the DConvert utility. This is done by clicking the DConvert's **Process Dial Plan File** button. For a detailed description of the DConvert utility, refer to the Product Reference Manual. You can load this *.dat file to the device using the Web interface (see 'Loading Auxiliary Files' on page 471), BootP & TFTP utility, or using the Auto-update mechanism from an external HTTP server.



Notes:

- Tel-to-IP routing is performed on the original source number if the parameter 'Tel to IP Routing Mode' is set to 'Route calls before manipulation'.
- Tel-to-IP routing is performed on the modified source number as defined in the Dial Plan file, if the parameter 'Tel To IP Routing Mode' is set to 'Route calls after manipulation'.
- Source number Tel-to-IP manipulation is performed on the modified source number as defined in the Dial Plan file.

18.7.3 Dial Plan Prefix Tags for IP-to-Tel Routing

The device supports the use of string labels (or "tags") in the external Dial Plan file for tagging incoming IP-to-Tel calls. The special "tag" is added as a prefix to the called party number, and then the Inbound IP Routing Table' uses this "tag" instead of the original prefix. Manipulation is then performed after routing in the Manipulation table, which strips the "tag" characters before sending the call to the endpoint.

This feature resolves the limitation of entries in the Inbound IP Routing Table' (IP-to-Tel call routing) for scenarios in which many different routing rules are required. For example, a city may have many different area codes, some for local calls and others for long distance calls (e.g. 425-202-xxxx for local calls, but 425-200-xxxx for long distance calls).

For using tags, the Dial Plan file is defined as follows:

- Number of dial plan (text)
- Dial string prefix (ranges can be defined in brackets)
- User-defined routing tag (text)



Note: Dial Plan Prefix Tags are not applicable to FXS and FXO interfaces.

The example configuration below assumes a scenario where multiple prefixes exist for local and long distance calls:

➤ **To use Dial Plan file routing tags:**

1. Load an *ini* file to the device that selects the Dial Plan index (e.g., 1) for routing tags, as shown below:

```
IP2TelTaggingDestDialPlanIndex = 1
```

2. Define the external Dial Plan file with two routing tags (as shown below):

- "LOCL" - for local calls
- "LONG" - for long distance calls

```
[ PLAN1 ]
42520[3-5],0,LOCL
425207,0,LOCL
42529,0,LOCL
425200,0,LONG
425100,0,LONG
```

Therefore, if an incoming IP call to destination prefix 425203 (for example) is received, the device adds the prefix tag "LOCL" (as specified in the Dial Plan file), resulting in the number "LOCL425203".

3. Assign the different tag prefixes to different Trunk Groups in the Inbound IP Routing Table' (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Routing** submenu > **IP to Trunk Group Routing**):
 - The Dest. Phone Prefix' field is set to the value "LOCL" and this rule is assigned to a local Trunk Group (e.g. Trunk Group ID 1).
 - The Dest. Phone Prefix' field is set to the value "LONG" and this rule is assigned to a long distance Trunk Group (e.g. Trunk Group ID 2).

Figure 18-33: Configuring Dial Plan File Label for IP-to-Tel Routing

Routing Index: 1-12						
IP To Tel Routing Mode: Route calls before manipulation						
	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Hunt Group ID
1			LOCL			1
2			LONG			2

The above routing rules are configured to be performed before manipulation (described in the step below).

4. Configure manipulation in the Destination Phone Number Manipulation Table for IP to Tel Calls table (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** submenu > **Dest Number IP->Tel**) for removing the first four characters of the called party number "tag" (in our example, "LOCL" and "LONG"):
 - The Destination Prefix' field is set to the value "LOCL" and the 'Stripped Digits From Left' field is set to '4'.
 - The Destination Prefix' field is set to the value "LONG" and the 'Stripped Digits From Left' field is set to '4'.

Figure 18-34: Configuring Manipulation for Removing Label

Index	Destination Prefix	Source Prefix	Source IP Address	Stripped Digits From Left
1	LOCL	*	*	4
2	LONG	*	*	4

18.8 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



Note: If the alternative routing destination is the device itself, the call can be configured to be routed back to one of the device's Trunk Groups and thus, back to the PSTN (PSTN Fallback).

18.8.1 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 Outbound IP Routing Table (described in 'Configuring the Outbound IP Routing Table' on page 269). 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.

18.8.2 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.

18.8.3 PSTN Fallback

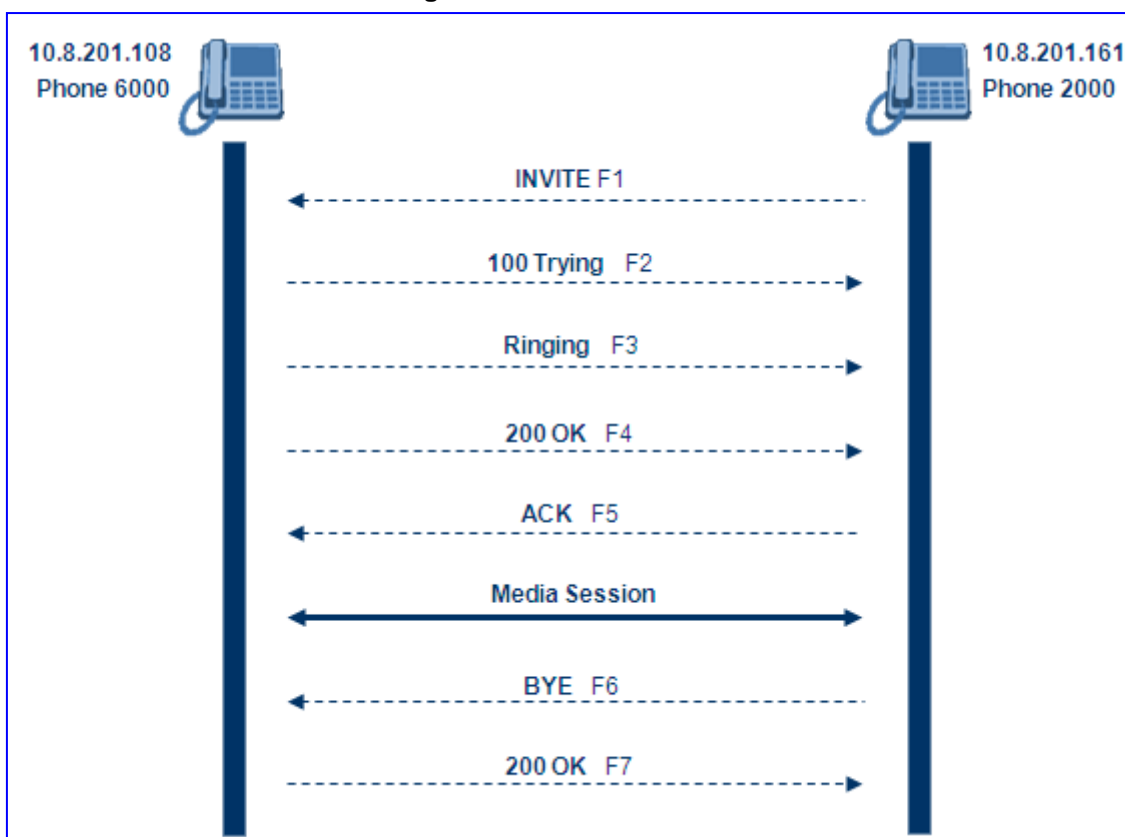
The PSTN Fallback feature enables the device to redirect PSTN originated calls back to the legacy PSTN network if a destination IP route is unsuitable (disallowed) for voice traffic at a specific time. To enable PSTN fallback, assign the device's IP address as an alternative route to the desired prefixes. Note that calls (now referred to as IP-to-Tel calls) can be re-routed to a specific Trunk Group using the Routing parameters (see 'Configuring iptotelrouteM1K>' on page 277).

18.9 SIP Call Routing Examples

18.9.1 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 18-35: 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/Mediant 1000/v.6.40.010.006
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/Mediant 1000/v.6.40.010.006
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/Mediant 1000/v.6.40.010.006
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/Mediant 1000/v.6.40.010.006
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/Mediant 1000/v.6.40.010.006
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/Mediant 1000/v.6.40.010.006
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/Mediant 1000/v.6.40.010.006
CSeq: 18154 BYE
Supported: 100rel,em
Content-Length: 0

```

18.9.2 SIP Message Authentication Example

The device supports basic and digest (MD5) authentication types, according to SIP RFC 3261 standard. A proxy server might require authentication before forwarding an INVITE message. A Registrar/Proxy server may also require authentication for client registration. A proxy replies to an unauthenticated INVITE with a 407 Proxy Authorization Required response, containing a Proxy-Authenticate header with the form of the challenge. After sending an ACK for the 407, the user agent can then re-send the INVITE with a Proxy-Authorization header containing the credentials.

User agents, Redirect or Registrar servers typically use 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/Mediant 1000/v.6.40.010.006
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/Mediant 1000/v.6.40.010.006
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
```

18.9.3 Establishing a Call between Two Devices

This section provides an example on configuring two AudioCodes' devices with FXS interfaces for establishing call communication. This setup enables the establishment of calls between telephones connected to the same device, and between the two devices.

This example assumes the following:

- IP address of the first device is 10.2.37.10 and its endpoint numbers are 101 to 104.
- IP address of the second device is 10.2.37.20 and its endpoint numbers are 201 to 204.
- SIP Proxy is not used. Internal call routing is performed using the device's Outbound IP Routing Table.

➤ **To configure the two devices for call communication:**

1. For the *first* device (10.2.37.10), in the Trunk Group Table page (see Configuring Trunk Group Table on page 249), assign the phone numbers 101 to 104 to the device's endpoints.

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID
1	Module 3 FXS	1	1	1-4	101	0

2. For the *second* device (10.2.37.20), in the Trunk Group Table page, assign the phone numbers 201 to 204 to the device's endpoints.

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID
1	Module 3 FXS	1	1	1-4	201	0

3. Configure the following for *both* devices:

In the Outbound IP Routing Table page (see 'Configuring Outbound IP Routing Table' on page 269), 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.

	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address	Dest. IP Group ID
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.

18.9.4 Trunk-to-Trunk Routing Example

This example describes two devices, each interfacing with the PSTN through four E1 spans. Device **A** is configured to route all incoming Tel-to-IP calls to Device **B**. Device **B** generates calls to the PSTN on the same E1 trunk on which the call was originally received (in Device **A**).

- Device **A** IP address: 192.168.3.50
- Device **B** IP address: 192.168.3.51

The *ini* file parameters configuration for devices **A** and **B** are as follows:

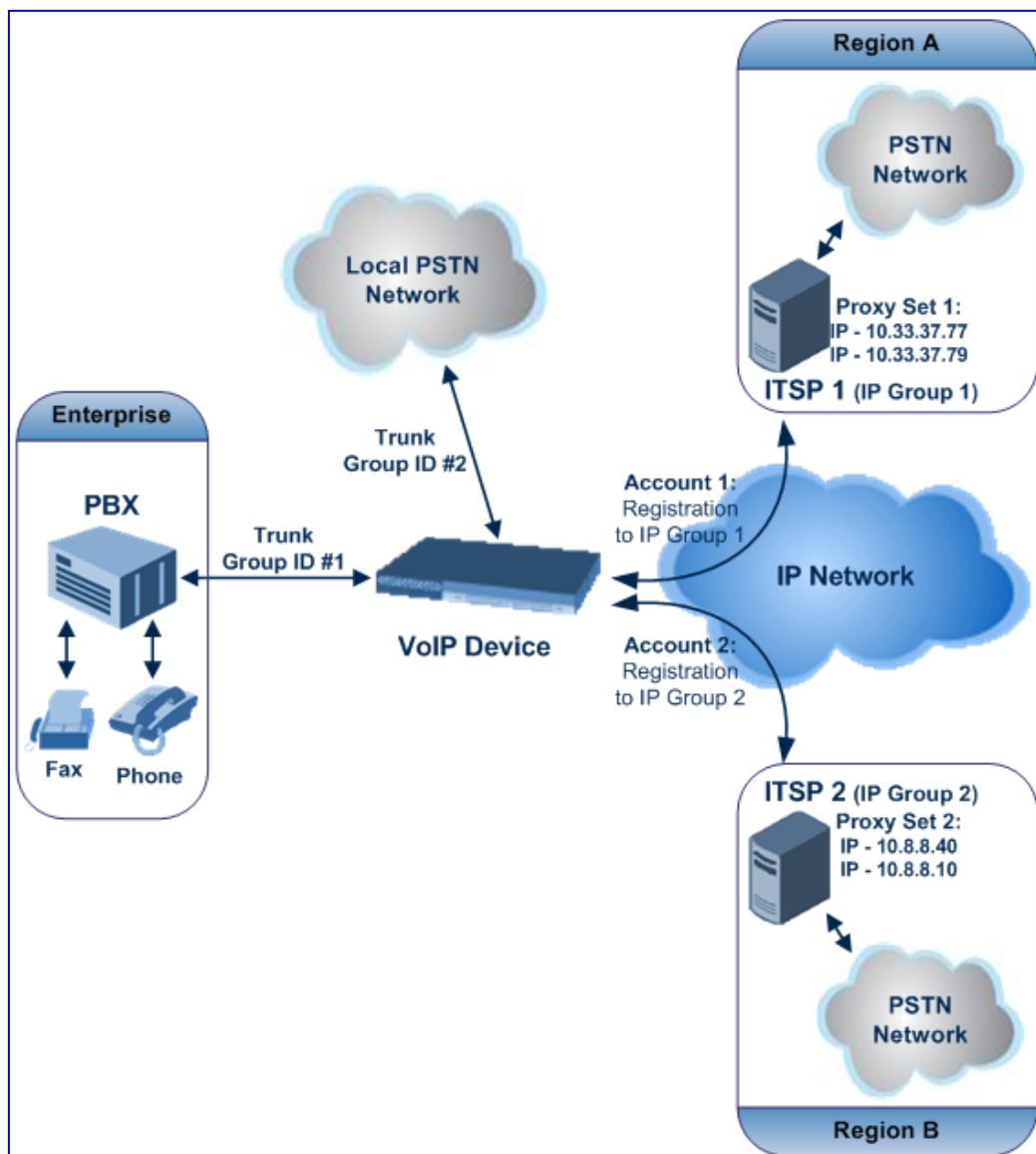
1. At both devices, define four Trunk Groups, each with 30 B-channels:
 - TrunkGroup_1 = 0/1-31,1000
 - TrunkGroup_2 = 1/1-31,2000
 - TrunkGroup_3 = 2/1-31,3000
 - TrunkGroup_4 = 3/1-31,4000
2. At Device **A**, add the originating Trunk Group ID as a prefix to the destination number for Tel-to-IP calls:
AddTrunkGroupAsPrefix = 1
3. At Device **A**, route all incoming PSTN calls starting with prefixes 1, 2, 3, and 4, to the IP address of Device **B**:
 - Prefix = 1, 192.168.3.51
 - Prefix = 2, 192.168.3.51
 - Prefix = 3, 192.168.3.51
 - Prefix = 4, 192.168.3.51

Note: You can also define Prefix = *,192.168.3.51, instead of the four lines above.
4. At Device **B**, route IP-to-PSTN calls to Trunk Group ID according to the first digit of the called number:
 - PSTNPrefix = 1,1
 - PSTNPrefix = 2,2
 - PSTNPrefix = 3,4
 - PSTNPrefix = 4,4
5. At Device **B**, remove the first digit from each IP-to-PSTN number before it is used in an outgoing call: NumberMapIP2Tel = *,1.

18.9.5 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's PBX and two Internet Telephony Service Providers (ITSP), using the device.

Scenario: In this example, the Enterprise wishes to connect its TDM PBX to two different ITSPs, by implementing the device in its network environment. It's main objective is for the device to route Tel-to-IP calls to these ITSPs according to a dial plan. The device is to register (on behalf of the PBX) to each ITSP, which implements two servers for redundancy and load balancing. The Register messages must use different URI's in the From, To, and Contact headers per ITSP. In addition, all calls dialed from the Enterprise PBX with prefix '02' is sent to the local PSTN. The figure below illustrates this example setup:



➤ **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 198), 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 18-36: Configuring Proxy Set ID #1 in the Proxy Sets Table Page

The screenshot shows the configuration for Proxy Set ID #1. At the top, 'Proxy Set ID' is set to 1. Below is a table with two columns: 'Proxy Address' and 'Transport Type'.

	Proxy Address	Transport Type
1	10.33.37.77	UDP
2	10.33.37.79	TCP
3		
4		
5		

Below the table are several configuration options:

- Enable Proxy Keep Alive: Using Options
- Proxy Keep Alive Time: 60
- Proxy Load Balancing Method: Round Robin
- Is Proxy Hot Swap: No
- Proxy Redundancy Mode: (-1) - Not Configured
- SRD Index: 1

3. In the IP Group Table page (see 'Configuring IP Groups' on page 193), configure the two IP Groups #1 and #2. Assign Proxy Sets #1 and #2 to IP Groups #1 and #2 respectively.

Figure 18-37: Configuring IP Groups #1 and #2 in the IP Group Table Page

The screenshot shows the configuration for IP Group #1. At the top, 'Index' is set to 1. Below is the 'Common Parameters' section:

Type	
Description	ITSP_1
Proxy Set ID	1
SIP Group Name	
Contact User	
IP Profile ID	0

- In the Trunk Group Table page, enable the Trunks connected between the Enterprise's PBX and the device (Trunk Group ID #1), and between the local PSTN and the device (Trunk Group ID #2).

Figure 18-38: Assigning Trunks to Trunk Group ID #1

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 PRI	1	1	1-30	1100	1	0
2	Module 1 PRI	2	2	1-30	2200	2	0

- In the Trunk Group Settings page, configure 'Per Account' registration for Trunk Group ID #1 (without serving IP Group)

Figure 18-39: Configuring Trunk Group #1 for Registration per Account in Trunk Group Settings Page

Trunk Group ID	Channel Select Mode	Registration Mode	Serving IP Group ID	Gateway Name	Contact User
1	Cyclic Ascending	Per Account			username

- In the Account Table page, configure the two Accounts for PBX trunk registration to ITSPs using the same Trunk Group (i.e., ID #1), but different serving IP Groups #1 and #2. For each account, define user name, password, and hostname, and ContactUser. The Register messages use different URI's (Hostname and ContactUser) in the From, To, and Contact headers per ITSP. Enable registration for both accounts.

Figure 18-40: Configuring Accounts for PBX Registration to ITSPs in Account Table Page

Index	ServedTrunkGroup	ServingIPGroup	Username	Password	HostName	Register	ContactUser
1	1	1	user1	1234	ITSP1	1	ITSP1user
2	1	2	user2	5555	ITSP2	1	ITSP2user

- In the Inbound IP Routing Table page, configure IP-to-Tel routing for calls from ITSPs to Trunk Group ID #1 (see 1 below) and from the device to the local PSTN (see 2 below).

Figure 18-41: Configuring ITSP-to-Trunk Group #1 Routing in IP to Trunk Group Table Page

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IPGroup ID
1			*	*		1		
2			02	*		2		

- In the Outbound IP Routing Table page, configure Tel-to-IP routing rules for calls to ITSPs (see first entry below) and to local PSTN (see second and third entries below).

Figure 18-42: Configuring Tel-to-IP Routing to ITSPs in Tel to IP Routing Table Page

Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address	Port	Transport Type	Dest. IPGroup ID
1	0[3,4,5]	*			Not Configured	1
1	0[6,7,8]	*			Not Configured	2
1	02	*	10.13.4.13		Not Configured	

18.10 IP-to-IP Routing Application

The device's supports IP-to-IP VoIP call routing (or SIP Trunking). The IP-to-IP call routing application enables enterprises to seamlessly connect their IP-based PBX (IP-PBX) to SIP trunks, typically provided by an Internet Telephony Service Provider (ITSP). By implementing the device, enterprises can then communicate with PSTN networks (local and overseas) through ITSP's, which interface directly with the PSTN. Therefore, the IP-to-IP application enables enterprises to replace the bundles of physical PSTN wires with SIP trunks provided by ITSP's and use VoIP to communicate within and outside the enterprise network using its standard Internet connection. At the same time, the device can also provide an interface with the traditional PSTN network, enabling PSTN fallback in case of IP connection failure with the ITSP's.

In addition, the device supports multiple SIP Trunking. This can be useful in scenarios where if a connection to one ITSP fails, the call can immediately be transferred to another ITSP. In addition, by allowing multiple SIP trunks where each trunk is designated a specific ITSP, the device can route calls to an ITSP based on call destination (e.g., country code).

Therefore, in addition to providing VoIP communication within an enterprise's LAN, the device allows the enterprise to communicate outside of the corporate LAN using SIP Trunking. This includes remote (roaming) IP-PBX users, for example, employees using their laptops to communicate with one another from anywhere in the world such as at airports.

The IP-to-IP application can be implemented by enterprises in the following example scenarios:

- VoIP between an enterprise's headquarters and remote branch offices
- VoIP between an enterprise and the PSTN via an ITSP

The IP-to-IP call routing capability is feature-rich, allowing interoperability with different ITSP's or service providers:

- Easy and smooth integration with multiple ITSP SIP trunks.
- Supports SIP registration and authentication with ITSP servers (on behalf of the enterprise's IP telephony system) even if the enterprise's IP telephony system does not support registration and authentication.
- Supports SIP-over-UDP, SIP-over-TCP, and SIP-over-TLS transport protocols, one of which is generally required by the ITSP.
- Provides alternative routing to different destinations (to another ITSP or the PSTN) when the connection with an ITSP network is down.
- Provides fallback to the legacy PSTN telephone network upon Internet connection failure.
- Provides Transcoding from G.711 to G.729 coder with the ITSP for bandwidth reduction.
- Supports SRTP, providing voice traffic security toward the ITSP.
- IP-to-IP routing can be used in combination with the regular Gateway application. For example, an incoming IP call can be sent to an E1/T1 span or it can be forwarded to an IP destination.

Therefore, the device provides the ideal interface between enterprises' IP-PBX's and ITSP SIP trunks.

In the IP-to-IP application, SIP Methods\Responses are handled and terminated at each leg independently:

- Initiating Dialog INVITE: terminated at one leg and initiated on the other leg, 180\182\183\200\4xx uses the same logic and same limitations, in some cases the result may be a different response code.
- OPTIONS: terminated at each leg independently.

- INFO: only specific INFO's (such as DTMF) are handled; other types are omitted.
- UPDATE: terminated at each leg independently and may cause only changes in the RTP flow - Hold/Retrieve are the only exceptions that traverse the two legs.
- ReINVITE: terminated at each leg independently and may cause only changes in the RTP flow - Hold/Retrieve are the only exceptions that traverse the two legs.
- PRACK: terminated at each leg independently.
- REFER (within a dialog): terminated at each leg independently.
- 3xx Responses: terminated at each leg independently.
- 401/407 Responses to initial INVITE: in case the B2B session is associated with an Account, the responses is terminated at the receiving leg; in other cases, the responses are passed transparently.
- REGISTER: handled only in cases associated with a USER IP Group - Contact/To/From specific parameters are omitted.

18.10.1 Theory of Operation

The device's IP-to-IP SIP session is performed by implementing Back-to-Back User Agent (B2BUA). The device acts as a user agent for both ends (*legs*) of the SIP call (from call establishment to termination). The session negotiation is performed independently for each call leg, using global parameters such as coders or using IP Profiles associated with each call leg to assign different configuration behaviors for these two IP-to-IP call legs.

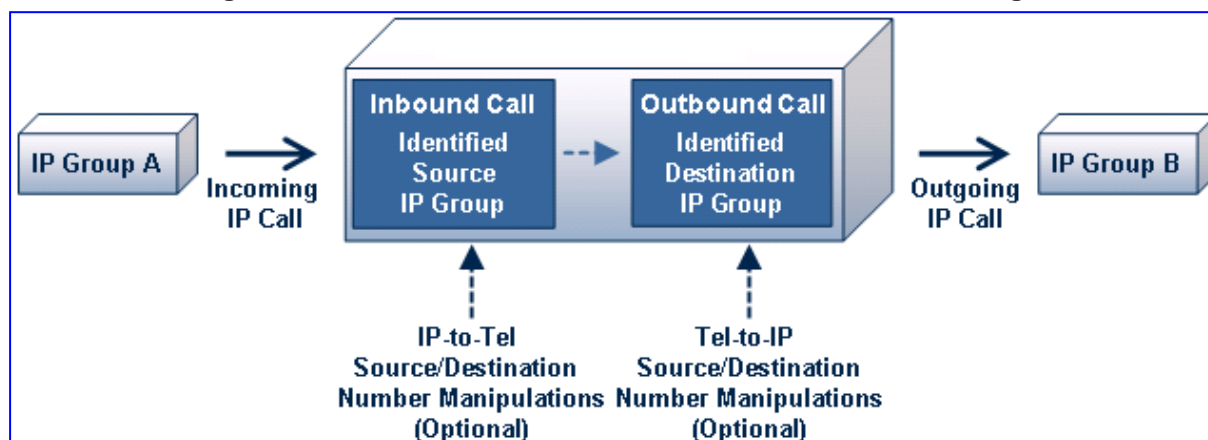
If transcoding is required, the RTP streams for IP-to-IP calls traverse through the device and two DSP channels are allocated per IP-to-IP session. Therefore, the maximum number of media channels that can be designated for IP-to-IP call routing is 120 (corresponding to 60 IP-to-IP sessions). If transcoding is not needed, the device supports up to 150 IP-to-IP SIP sessions (without using DSP channels).

RTP-to-SRTP interworking requires one DSP channel. Therefore, the device supports up to 120 RTP-to-SRTP SIP sessions (same number as RTP-to-RTP SIP sessions).

The device also supports NAT traversal for SIP clients behind NAT, where the device is defined with a global IP address.

The figure below provides a simplified illustration of the device's handling of IP-to-IP call routing:

Figure 18-43: Basic Schema of the Device's IP-to-IP Call Handling



The basic IP-to-IP call handling process can be summarized as follows:

1. Incoming IP calls are identified as belonging to a specific logical entity in the network (referred to as a *Source IP Group*), according to Inbound IP Routing rules.
2. The Source IP Group is associated with a specific IP Group (*Destination IP Group*), and then sent to the appropriate destination address (defined by a *Proxy Set*) associated with this Destination IP Group.

- Number manipulation can be performed at both legs (inbound and outbound).

The following subsections discuss the main terms associated with the IP-to-IP call routing application.

18.10.1.1 Proxy Sets

A Proxy Set is a group of up to five Proxy servers (for Proxy load balancing and redundancy), defined by IP address or fully qualified domain name (FQDN). The Proxy Set is assigned to IP Groups (of type SERVER only), representing the address of the IP Group to where the device sends the INVITE message (**destination** of the call). Typically, for IP-to-IP call routing, two Proxy Sets are defined for call destination – one for each leg (i.e., each IP Group) of the call (i.e., both directions).

18.10.1.2 IP Groups

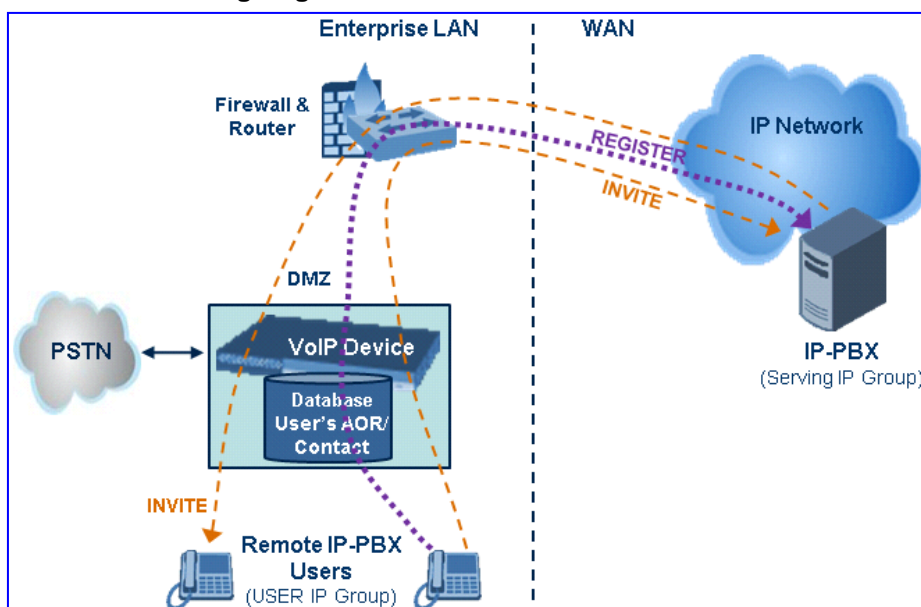
An IP Group represents a logical SIP entity in the device's network environment such as an ITSP SIP trunk, ITSP Proxy/Registrar server, IP-PBX, or remote IP-PBX users. The address of the IP Group is typically defined by the Proxy Set that is assigned to it.

The opposite legs of the call are each presented by an IP Group: one being a *Serving* IP Group; the other the *Served* IP Group. The Serving IP Group depicts the IP Group (e.g., ITSP) that provides service ("serves") to the Served IP Group (e.g., IP-PBX). This is the IP Group to where the device sends INVITE messages received from the Served IP Group as well as REGISTER messages for registering on behalf of the Served IP Group.

In addition, IP Groups can be *SERVER* or *USER* type. In SERVER IP Groups (e.g., ITSP or IP-PBX), the destination address (defined by the Proxy Set) is known. In contrast, USER IP Groups represents groups of users whose location is dynamically obtained by the device when REGISTER requests and responses traverse (or are terminated) by the device. Generally, these are remote IP-PBX users (e.g., IP phones and soft phones).

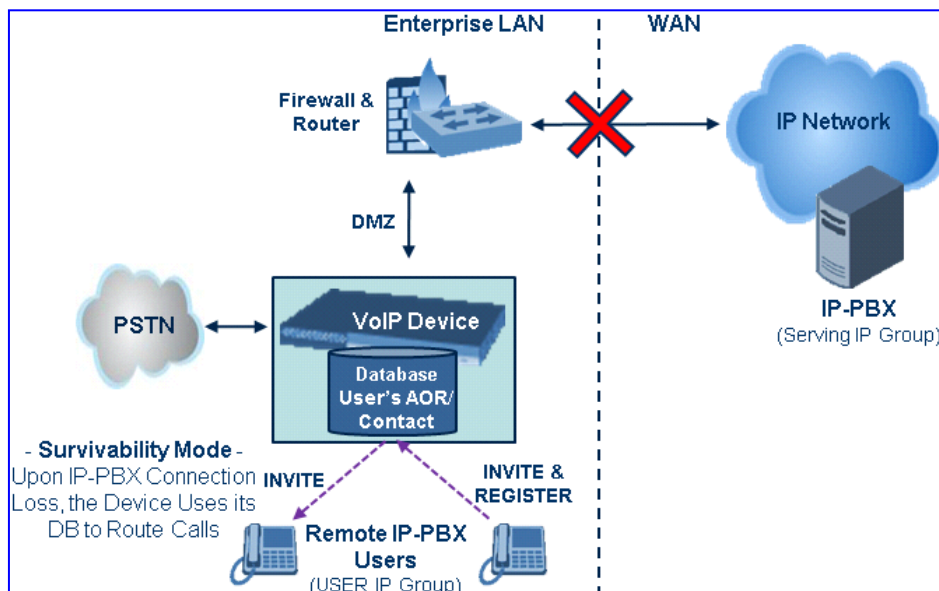
For registrations of USER IP Groups, the device updates its internal database with the AOR and Contacts of the users (refer to the figure below) Digest authentication using SIP 401/407 responses (if needed) is performed by the Serving IP Group (e.g., IP-PBX). The device forwards these responses directly to the remote SIP users. For a call to a registered remote user, the device searches its dynamic database (by using the Request URI) for an entry that matches a registered AOR or Contact. Once an entry is found, the IP destination is obtained and a SIP request is then sent to this user.

Figure 18-44: IP-to-IP Routing/Registration/Authentication of Remote IP-PBX Users (Example)



The device also supports the IP-to-IP call routing Survivability mode feature (refer to the figure below) for USER IP Groups. The device records (in its database) REGISTER messages sent by the clients of the USER IP Group. If communication with the Serving IP Group (e.g., IP-PBX) fails, the USER IP Group enters into Survivability mode in which the device uses its database for routing calls between the clients of the USER IP Group. The RTP packets between the clients traverse through the device. When the Serving IP Group is available again, the device returns to normal mode, sending INVITE and REGISTER messages to the Serving IP Group.

Figure 18-45: IP-to-IP Routing for IP-PBX Remote Users in Survivability Mode (Example)



18.10.1.3 Inbound and Outbound IP Routing Rules

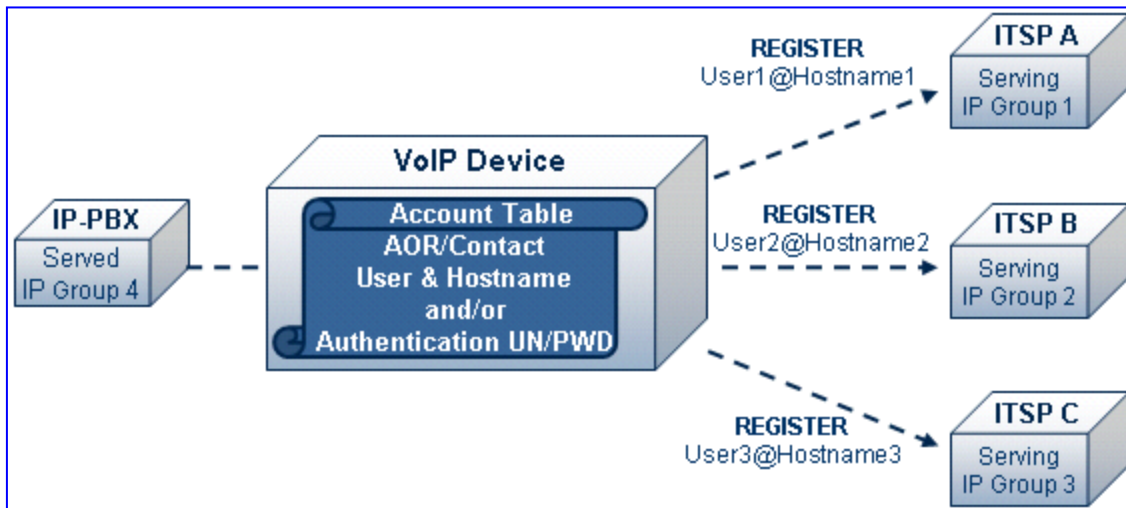
The device's IP-to-IP call routing is performed using the following two routing rule stages:

1. **Inbound IP Routing Mapping Rule:** Identifies the received call as an IP-to-IP call based on various characteristics such as the call's source IP address, and assigns it to an IP Group.
2. **Outbound IP Routing Mapping Rule:** Determines the destination (i.e., IP address) to where the incoming call (classified to a specific IP Group by the Inbound IP Routing rules) is finally routed. The destination address is typically depicted by another IP Group (destination IP Group) and therefore, the call is sent to the IP address that is defined in the Proxy Set associated with this IP Group. If the destination is a USER IP Group, the device searches for a match between the request URI (of the received INVITE) to an AOR registration record in the device's internal database. If a match is found, the INVITE is sent to the IP address of the registered contact.

18.10.1.4 Accounts

Accounts are used by the device to register to a Serving IP Group (e.g., an ITSP) on behalf of a Served IP Group (e.g., IP-PBX). This is necessary for ITSP's that require registration to provide services. Accounts are also used for defining user name/password for digest authentication (with or without registration) if required by the ITSP. Multiple Accounts per Served IP Group can be configured for registration to more than one Serving IP Group (e.g., an IP-PBX that requires registering to multiple ITSP's).

Figure 18-46: Registration with Multiple ITSP's on Behalf of IP-PBX



18.10.2 IP-to-IP Routing Configuration Example

This section provides step-by-step procedures for configuring IP-to-IP call routing. These procedures are based on the setup example described below. In this example, the device serves as the communication interface between the enterprise's IP-PBX (located on the LAN) and the following network entities:

- ITSP SIP trunks (located on the WAN)
- Remote IP-PBX users (located on the WAN)
- Local PSTN network

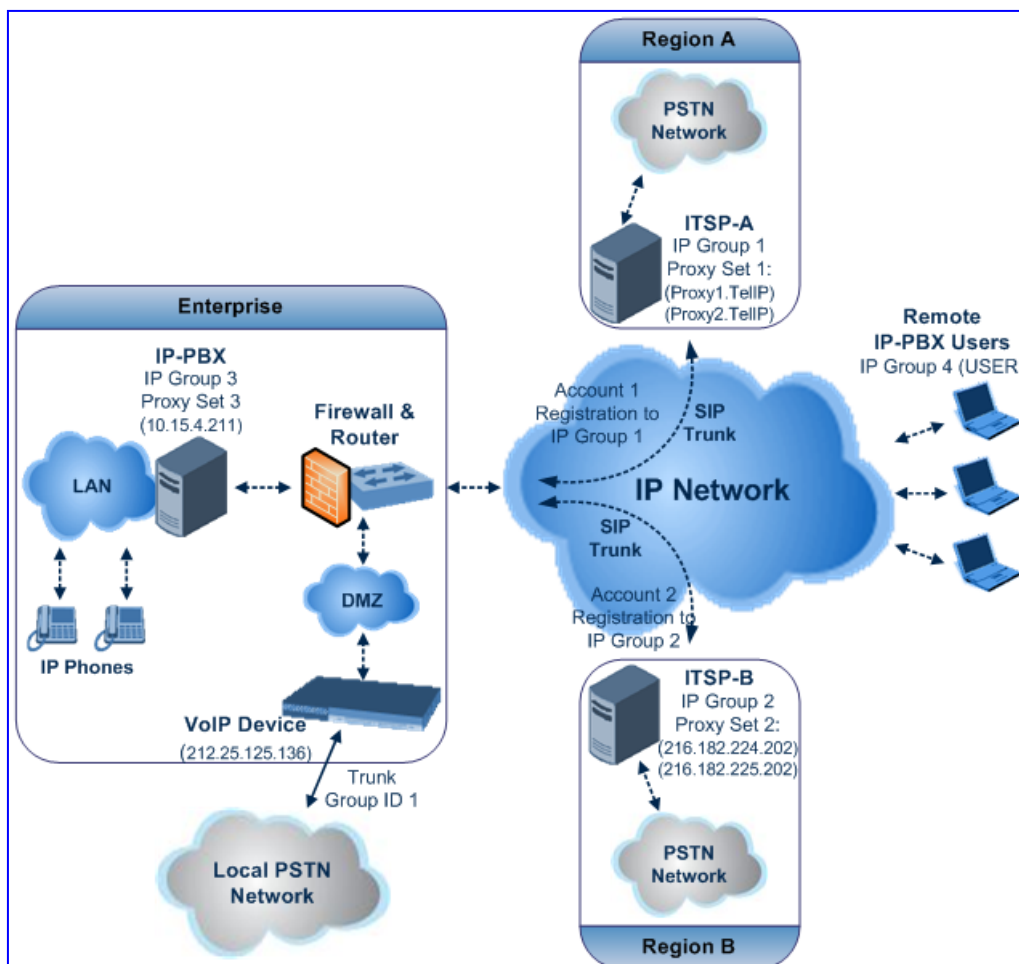
Calls from the Enterprise are routed according to destination.

This example assumes the following:

- The device has the public IP address 212.25.125.136 and is connected to the enterprise's firewall/NAT demilitarized zone (DMZ) network, providing the interface between the IP-PBX, and two ITSP's and the local PSTN.
- The enterprise has an IP-PBX located behind a Firewall/NAT:
 - IP-PBX IP address: 10.15.4.211
 - Transport protocol: UDP
 - Voice coder: G.711
 - IP-PBX users: 4-digit length extension number and served by two ITSPs.
 - The enterprise also includes remote IP-PBX users that communicate with the IP-PBX via the device. All dialed calls from the IP-PBX consisting of four digits starting with digit "4" are routed to the remote IP-PBX users.
- Using SIP trunks, the IP-PBX connects (via the device) to two different ITSP's:
 - **ITSP-A:**
 - ◆ Implements Proxy servers with fully qualified domain names (FQDN): "Proxy1.ITSP-A" and "Proxy2.ITSP-B", using TLS.
 - ◆ Allocates a range of PSTN numbers beginning with +1919, which is assigned to a range of IP-PBX users.
 - ◆ Voice coder: G.723.
 - **ITSP-B:**
 - ◆ Implements Proxy servers with IP addresses 216.182.224.202 and 216.182.225.202, using TCP.
 - ◆ Allocates a range of PSTN numbers beginning with 0200, which is assigned to a range of IP-PBX users.
 - ◆ Voice coder: G.723.
- Registration and authentication is required by both ITSP's, which is performed by the device on behalf of the IP-PBX. The SIP REGISTER messages use different URI's (host name and contact user) in the From, To, and Contact headers per ITSP as well as username and password authentication.
- Outgoing calls from IP-PBX users are routed according to destination:
 - If the calls are dialed with the prefix "+81", they are routed to ITSP-A (Region A).
 - If the calls are dialed with the prefix "9", they are routed to the local PSTN network.
 - For all other destinations, the calls are routed to ITSP-B.
- The device is also connected to the PSTN through a traditional T1 ISDN trunk for local incoming and outgoing calls. Calls dialed from the enterprise's IP-PBX with prefix '9' are sent to the local PSTN. In addition, in case of Internet interruption and loss of connection with the ITSP trunks, all calls are rerouted to the PSTN.

The figure below provides an illustration of this example scenario:

Figure 18-47: SIP Trunking Setup Scenario Example



The steps for configuring the device according to the scenario above can be summarized as follows:

- Enable the IP-to-IP feature (see 'Step 1: Enable the IP-to-IP Capabilities' on page 358).
- Configure the number of media channels (see 'Step 2: Configure the Number of Media Channels' on page 358).
- Configure a Trunk Group for interfacing with the local PSTN (see 'Step 3: Define a Trunk Group for the Local PSTN' on page 359).
- Configure Proxy Sets (see 'Step 4: Configure the Proxy Sets' on page 359).
- Configure IP Groups (see 'Step 5: Configure the IP Groups' on page 361).
- Configure Registration Accounts (see 'Step 6: Configure the Account Table' on page 364).
- Configure IP Profiles (see 'Step 7: Configure IP Profiles for Voice Coders' on page 365).
- Configure inbound IP routing rules (see 'Step 8: Configure Inbound IP Routing' on page 367).
- Configure outbound IP routing rules (see 'Step 9: Configure Outbound IP Routing' on page 368).
- Configure destination phone number manipulation (see 'Step 10: Configure Destination Phone Number Manipulation' on page 370).

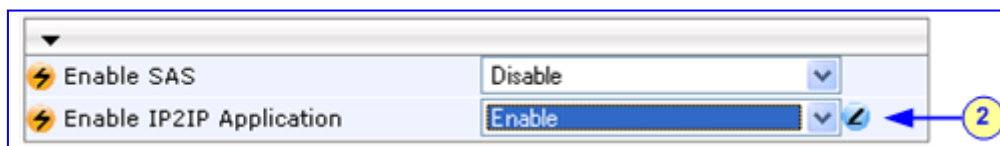
18.10.2.1 Step 1: Enable the IP-to-IP Capabilities

This step describes how to enable the device's IP-to-IP application.

➤ **To enable IP-to-IP capabilities:**

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** submenu > **Applications Enabling**).
2. From the 'Enable IP2IP Application' drop-down list, select **Enable**, as shown below:

Figure 18-48: Enabling the IP2IP Application



Note: For the IP-to-IP feature, the device must also be installed with the appropriate Software Upgrade Feature Key.

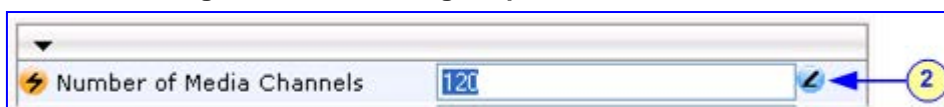
18.10.2.2 Step 2: Configure the Number of Media Channels

The number of media channels represents the number of digital signaling processors (DSP) channels that the device allocates to IP-to-IP calls. The remaining DSP channels can be used for PSTN calls. Two IP media channels are used per IP-to-IP call. Therefore, the maximum number of media channels that can be designated for IP-to-IP call routing is 120 (corresponding to 60 IP-to-IP calls).

➤ **To configure the number of media channels:**

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

Figure 18-49: Defining Required Media Channels



2. In the 'Number of Media Channels' field, enter the required number of media channels (in the example above, "120" to enable up to 60 IP-to-IP calls).
3. Click **Submit**.
4. Save the settings to flash memory ("burn") and reset the device (see 'Saving Configuration' on page 470).

18.10.2.3 Step 3: Define a Trunk Group for the Local PSTN

For incoming and outgoing local PSTN calls with the IP-PBX, you need to define the Trunk Group ID (#1) for the T1 ISDN trunk connecting between the device and the local PSTN. This Trunk Group is also used for alternative routing to the legacy PSTN network in case of a loss of connection with the ITSP's.

➤ **To configure the Trunk Group for local PSTN:**

1. Open the Trunk Group Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Trunk Group** > **Trunk Group**).
2. Configure Trunk Group ID #1 (as shown in the figure below):
 - From the 'From Trunk' and 'To Trunk' drop-down lists, select **1** to indicate Trunk 1 for this Trunk Group.
 - In the 'Channels' field, enter the Trunk channels or ports assigned to the Trunk Group (e.g. 1-31 for E1 and 1-24 for T1).
 - In the 'Phone Number' field, enter any phone number (logical) for this Trunk (e.g. 1000).
 - In the 'Trunk Group ID' field, enter "1" as the ID for this Trunk Group.

Add Phone Context As Prefix		Disable					
Trunk Group Index		1-12					

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 PRI	1	1	1-31	1000	1	
2							

3. Configure the Trunk in the Trunk Settings page (**Configuration** tab > **VoIP** menu > **PSTN** submenu > **Trunk Settings**).

18.10.2.4 Step 4: Configure the Proxy Sets

This step describes how to configure the following Proxy Sets:

- Proxy Set ID #1 defined with two FQDN's for ITSP-A
- Proxy Set ID #2 defined with two IP addresses for ITSP-B
- Proxy Set ID #3 defined with an IP address for the IP-PBX

The Proxy Sets represent the actual destination (IP address or FQDN) to which the call is routed. These Proxy Sets are later assigned to IP Groups (see 'Step 5: Configure the IP Groups' on page 361).

➤ **To configure the Proxy Sets:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).
2. Configure Proxy Set ID #1 for ITSP-A:
 - a. From the 'Proxy Set ID' drop-down list, select **1**.
 - b. In the 'Proxy Address' column, enter the FQDN of ITSP-A SIP trunk Proxy servers (e.g., Proxy1.ITSP-A and Proxy2. ITSP-A).
 - c. From the 'Transport Type' drop-down list corresponding to the Proxy addresses entered above, select **TLS**.

- d. In the 'Enable Proxy Keep Alive' drop-down list, select **Using Options**, and then in the 'Proxy Load Balancing Method' drop-down list, select **Round Robin**.

Figure 18-50: Proxy Set ID #1 for ITSP-A

Proxy Address	Transport Type
1 Proxy1.ITSP-A	TLS
2 Proxy2.ITSP-A	TLS
3	
4	
5	

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Round Robin
Is Proxy Hot Swap	No
Proxy Redundancy Mode	(-1) - Not Configured
SRD Index	0

3. Configure Proxy Set ID #2 for ITSP-B:
 - a. From the 'Proxy Set ID' drop-down list, select **2**.
 - b. In the 'Proxy Address' column, enter the IP addresses of the ITSP-B SIP trunk (e.g., 216.182.224.202 and 216.182.225.202).
 - c. From the 'Transport Type' drop-down list corresponding to the IP address entered above, select **UDP**.
 - d. In the 'Enable Proxy Keep Alive' drop-down list, select "Using Options", and then in the 'Proxy Load Balancing Method' drop-down list, select **Round Robin**.

Figure 18-51: Proxy Set ID #2 for ITSP-B

Proxy Address	Transport Type
1 216.182.224.202	UDP
2 216.182.225.202	UDP
3	
4	
5	

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Round Robin
Is Proxy Hot Swap	No
Proxy Redundancy Mode	(-1) - Not Configured
SRD Index	0

4. Configure Proxy Set ID #3 for the IP-PBX:
 - a. From the 'Proxy Set ID' drop-down list, select **3**.
 - b. In the 'Proxy Address' column, enter the IP address of the IP-PBX (e.g., 10.15.4.211).
 - c. From the 'Transport Type' drop-down list corresponding to the IP address entered above, select **UDP**".
 - d. In the 'Enable Proxy Keep Alive' drop-down list, select **Using Options** – this is used in Survivability mode for remote IP-PBX users.

Figure 18-52: Proxy Set ID #3 for the IP-PBX

The screenshot shows the configuration for Proxy Set ID #3. The 'Proxy Set ID' is set to 3. The table below lists proxy addresses and transport types. The first row is populated with IP address 10.15.4.211 and transport type UDP. The 'Enable Proxy Keep Alive' setting is set to 'Using Options'.

Proxy Address	Transport Type
1 10.15.4.211	UDP
2	
3	
4	
5	

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	(-1) - Not Configured
SRD Index	0

18.10.2.5 Step 5: Configure the IP Groups

This step describes how to create the IP Groups for the following entities in the network:

- ITSP-A SIP trunk
- ITSP-B SIP trunk
- IP-PBX
- IP-PBX remote users

These IP Groups are later used by the device for routing calls.

➤ To configure the IP Groups:

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **IP Group Table**).
2. Define IP Group #1 for ITSP-A:
 - a. From the 'Type' drop-down list, select **SERVER**.
 - b. In the 'Description' field, type an arbitrary name for the IP Group (e.g., ITSP A).
 - c. From the 'Proxy Set ID' drop-down lists, select **1** (represents the IP addresses, configured in , for communicating with this IP Group).
 - d. In the 'SIP Group Name' field, enter the host name sent in the SIP Request From\To headers for this IP Group, as required by ITSP-A (e.g., RegionA).

- e. Contact User = name that is sent in the SIP Request's Contact header for this IP Group (e.g., ITSP-A).

Figure 18-53: Defining IP Group 1

Common Parameters	
Type	SERVER
Description	ITSP-A
Proxy Set ID	1
SIP Group Name	RegionA
Contact User	itsp_a
SRD	0
Media Realm	
IP Profile ID	0

Gateway Parameters	
Always Use Route Table	No
Routing Mode	Routing Table
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	

3. Define IP Group #2 for ITSP-B:
 - a. From the 'Type' drop-down list, select **SERVER**.
 - b. In the 'Description' field, type an arbitrary name for the IP Group (e.g., ITSP B).
 - c. From the 'Proxy Set ID' drop-down lists, select **2** (represents the IP addresses, configured in , for communicating with this IP Group).
 - d. In the 'SIP Group Name' field, enter the host name sent in SIP Request From\To headers for this IP Group, as required by ITSP-B (e.g., RegionB).
 - e. Contact User = name that is sent in the SIP Request Contact header for this IP Group (e.g., ITSP-B).

Figure 18-54: Defining IP Group 2

Common Parameters	
Type	SERVER
Description	ITSP-B
Proxy Set ID	2
SIP Group Name	RegionB
Contact User	itsp_b
SRD	0
Media Realm	
IP Profile ID	0

Gateway Parameters	
Always Use Route Table	No
Routing Mode	Routing Table
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	

4. Define IP Group #3 for the IP-PBX:
 - a. From the 'Type' drop-down list, select **SERVER**.
 - b. In the 'Description' field, type an arbitrary name for the IP Group (e.g., IP-PBX).
 - c. From the 'Proxy Set ID' drop-down lists, select **3** (represents the IP address, configured in , for communicating with this IP Group).
 - d. In the 'SIP Group Name' field, enter the host name that is sent in SIP Request From\To headers for this IP Group (e.g., IPPBX).
 - e. Contact User = name that is sent in the SIP Request Contact header for this IP Group (e.g., PBXUSER).

Figure 18-55: Defining IP Group 3

Common Parameters	
Index	3
Type	SERVER
Description	IP-PBX
Proxy Set ID	3
SIP Group Name	IPPBX
Contact User	pbxuser
SRD	0
Media Realm	
IP Profile ID	0
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Routing Table
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	

5. Define IP Group #4 for the remote IP-PBX users:
 - a. From the 'Type' drop-down list, select **USER**.
 - b. In the 'Description' field, type an arbitrary name for the IP Group (e.g., IP-PBX).
 - c. In the 'SIP Group Name' field, enter the host name that is used internal in the device's database for this IP Group (e.g., RemoteIPPBXusers).

- d. From the 'Serving IP Group ID' drop-down list, select **3** (i.e. the IP Group for the IP-PBX).

Figure 18-56: Defining IP Group 4



Note: No Serving IP Groups are defined for ITSP-A and ITSP-B. Instead, the Outbound IP Routing table (see 'Step 9: Configure Outbound IP Routing' on page 368) is used to configure outbound call routing for calls originating from these ITSP IP Groups.

18.10.2.6 Step 6: Configure the Account Table

The Account table is used by the device to register to an ITSP on behalf of the IP-PBX. As described previously, the ITSP's requires registration and authentication to provide service. For the example, the Served IP Group is the IP-PBX (IP Group ID #3) and the Serving IP Groups are the two ITSP's (IP Group ID's #1 and #2).

- **To configure the Account table:**
 1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Account Table**).

Figure 18-57: Defining Accounts for Registration

Index	Served Trunk Group	Served IP Group	Serving IP Group	Username	Password
1	-1	3	1	itsp_a	*
2	-1	3	2	itsp_b	*

Host Name	Register	Contact User	Application Type
regiona	Yes	ITSP-A	GW\IP2IP
regionb	Yes	ITSP-B	GW\IP2IP

2. Configure Account ID #1 for IP-PBX authentication and registration with ITSP-A:
 - In the 'Served IP Group' field, enter "3" to indicate that authentication is performed on behalf of IP Group #3 (i.e., the IP-PBX).
 - In the 'Serving IP Group' field, enter "1" to indicate that registration/authentication is with IP Group #1 (i.e., ITSP-A).
 - In the 'Username', enter the SIP username for authentication supplied by ITSP-A (e.g., itsp_a).
 - In the 'Password' field, enter the SIP password for authentication supplied by ITSP-A (e.g., 12345).
 - In the 'Register' field, enter "1" to enable registration with ITSP-A.
3. Configure Account ID #2 for IP-PBX registration) with ITSP-B Registrar server:
 - In the 'Served IP Group' field, enter "3" to indicate that registration is performed on behalf of IP Group #3 (i.e., the IP-PBX).
 - In the 'Serving IP Group' field, enter "2" to indicate that registration is with IP Group #3 (e.g., ITSP-B).
 - In the 'Username', enter the SIP username for the registration/authentication supplied by ITSP-B (e.g., itsp_b).
 - In the 'Password' field, enter the SIP password for registration/authentication supplied by ITSP-B (e.g., 11111).
 - In the 'Register' field, enter "1" to enable registration with ITSP-B.

18.10.2.7 Step 7: Configure IP Profiles for Voice Coders

Since different voice coders are used by the IP-PBX (G.711) and the ITSP's (G.723), you need to define two IP Profiles:

- Profile ID #1 - configured with G.711 for the IP-PBX
- Profile ID #2 - configured with G.723 for the ITSP's

These profiles are later used in the Inbound IP Routing table and Outbound IP Routing table.

➤ To configure IP Profiles for voice coders:

1. Open the Coder Group Settings page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **Coders Group Settings**)
2. Configure Coder Group ID #1 for the IP-PBX (as shown in the figure below):
 - a. From the 'Coder Group ID' drop-down list, select 1.
 - b. From the 'Coder Name' drop-down list, select **G.711A-law**.
 - c. Click **Submit**.

Figure 18-58: Defining Coder Group ID 1

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711A-law	20	64	8	Disabled

3. Configure Coder Group ID #2 for the ITSP's (as shown in the figure below):

- a. From the 'Coder Group ID' drop-down list, select **2**.
- b. From the 'Coder Name' drop-down list, select **G.723.1**.
- c. Click **Submit**.

Figure 18-59: Defining Coder Group ID 2

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.723.1	30	5.3	4	Disabled

4. Open the IP Profile Settings page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** submenu > **IP Profile Settings**).
5. Configure Profile ID #1 for the IP-PBX (as shown below):
 - a. From the 'Profile ID' drop-down list, select **1**.
 - b. From the 'Coder Group' drop-down list, select **Coder Group 1**.
 - c. Click **Submit**.

Figure 18-60: Defining IP Profile ID 1

Profile ID	1
Profile Name	IP-PBX
Common Parameters	
RTP IP DiffServ	46
Signaling DiffServ	40
Disconnect on Broken Connection	Yes
Coder Group	Coder Group 1
Remote RTP Base UDP Port	0
First Tx DTMF Option	Not Supported
Second Tx DTMF Option	Not Supported
Declare RFC 2833 in SDP	Yes
Add IE In SETUP	
Enable Hold	Enable

6. Configure Profile ID #2 for the ITSP's:
 - a. From the 'Profile ID' drop-down list, select **2**.
 - b. From the 'Coder Group' drop-down list, select **Coder Group 2**.
 - c. Click **Submit**.

18.10.2.8 Step 8: Configure Inbound IP Routing

This step defines how to configure the device for routing inbound (i.e., received) IP-to-IP calls. The table in which this is configured uses the IP Groups that you defined in 'Step 5: Configure the IP Groups' on page 361.

➤ **To configure inbound IP routing:**

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

Figure 18-61: Defining Inbound IP Routing Rules

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IPGroup ID
2			9	*	*	1	0	
3			*	*	10.15.4211	-1	1	3
4			+1919	*	*	-1	2	1
5			0200	*	*	-1	2	2
6	*	pbxremote	*	*	*	-1	0	4
7			*	*	10.15.4211	1	0	-1

2. **Index #1:** routes calls with prefix 9 (i.e., local calls) dialed from IP-PBX users to the local PSTN:
 - 'Dest Phone Prefix': enter "9" for the dialing prefix for local calls.
 - 'Trunk Group ID': enter "1" to indicate that these calls are routed to the Trunk (belonging to Trunk Group #1) connected between the device and the local PSTN network.
3. **Index #2:** identifies IP calls received from the IP-PBX as IP-to-IP calls and assigns them to the IP Group ID configured for the IP-PBX:
 - 'Dest Phone Prefix': enter the asterisk (*) symbol to indicate all destinations.
 - 'Source IP Address': enter the IP address of the IP-PBX (i.e., 10.15.4.211).
 - 'Trunk Group ID': enter "-1" to indicate that these calls are IP-to-IP calls.
 - 'IP Profile ID': enter "1" to assign these calls to Profile ID #1 to use G.711.
 - 'Source IP Group ID': enter "3" to assign these calls to the IP Group pertaining to the IP-PBX.
4. **Index #3:** identifies IP calls received from ITSP-A as IP-to-IP calls and assigns them to the IP Group ID configured for ITSP-A:
 - 'Dest Phone Prefix': ITSP-A assigns the Enterprise a range of numbers that start with +1919. Enter this prefix to indicate calls received from this ITSP.
 - 'Trunk Group ID': enter "-1" to indicate that these calls are IP-to-IP calls.
 - 'IP Profile ID': enter "2" to assign these calls to Profile ID #2 to use G.723.
 - 'Source IP Group ID': enter "1" to assign these calls to IP Group pertaining to ITSP-A.
5. **Index #4:** identifies IP calls received from ITSP-B as IP-to-IP calls and assigns them to the IP Group ID configured for ITSP-B:
 - 'Dest Phone Prefix': ITSP-B assigns the Enterprise a range of numbers that start with 0200. Enter this prefix to indicate calls coming from this ITSP.
 - 'Trunk Group ID': enter "-1" to indicate that these calls are IP-to-IP calls.
 - 'IP Profile ID': enter "2" to assign these calls to Profile ID #2 to use G.723.

- 'Source IP Group ID': enter "2" to assign these calls to IP Group pertaining to ITSP-B.
6. **Index #5:** identifies all IP calls received from IP-PBX remote users:
- 'Source Host Prefix': enter "PBXuser". This is the host name that appears in the From header of the Request URI received from remote IP-PBX users.
 - 'Trunk Group ID': enter "-1" to indicate that these calls are IP-to-IP calls.
 - 'Source IP Group ID': enter "4" to assign these calls to the IP Group pertaining to the remote IP-PBX users.
7. **Index #6:** is used for alternative routing. This configuration identifies all IP calls received from the IP-PBX and which can't reach the ITSP's servers (e.g. loss of connection with ITSP's) and routes them to the local PSTN network:
- 'Dest Phone Prefix': enter the asterisk (*) symbol to indicate all destinations.
 - 'Source IP Address': enter the IP address of the IP-PBX (i.e., 10.15.4.211).
 - 'Trunk Group ID': enter "1" to route these calls to the Trunk Group ID configured for the Trunk connected to the device and interfacing with the local PSTN.
 - 'Source IP Group ID': enter "-1" to indicate that these calls are not assigned to any source IP Group.

18.10.2.9 Step 9: Configure Outbound IP Routing

This step defines how to configure the device for routing outbound (i.e., sent) IP-to-IP calls. In our example scenario, calls from both ITSP's must be routed to the IP-PBX, while outgoing calls from IP-PBX users must be routed according to destination. If the calls are destined to the Japanese market, then they are routed to ITSP-B; for all other destinations, the calls are routed to ITSP-A. This configuration uses the IP Groups defined in 'Step 5: Configure the IP Groups' on page 361 and IP Profiles defined in 'Step 7: Configure IP Profiles for Voice Coders' on page 365.

➤ **To configure outbound IP routing rules:**

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

Figure 18-62: Defining Outbound IP Routing Rules

Src. IPGroupID	Src. Host Prefix	Dest Host Prefix	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address	Port	Transport Type	Dest. IPGroup ID	IP Profile ID
1				*	*	*		Not Configured	3	2
2				*	*	*		Not Configured	3	2
3			1	*	*	*		Not Configured	3	
4				+81	*	*		Not Configured	1	1
5				*	*	*		Not Configured	2	1
6				*##	*	*		Not Configured	4	1

2. **Index #1:** routes IP calls received from ITSP-A to the IP-PBX:
 - 'Source IP Group ID': select 1 to indicate received (inbound) calls identified as belonging to the IP Group configured for ITSP-A.
 - 'Dest Phone Prefix' and 'Source Phone Prefix' : enter the asterisk (*) symbol to indicate all destinations and callers respectively.
 - 'Dest IP Group ID': select 3 to indicate the destination IP Group to where these calls are sent, i.e., to the IP-PBX.
 - 'IP Profile ID': enter "2" to indicate the IP Profile configured for G.723.

3. **Index #2:** routes IP calls received from ITSP-B to the IP-PBX:
 - 'Source IP Group ID': select **2** to indicate received (inbound) calls identified as belonging to the IP Group configured for ITSP-B.
 - 'Dest Phone Prefix' and 'Source Phone Prefix': enter the asterisk (*) symbol to indicate all destinations and callers respectively.
 - 'Dest IP Group ID': select **3** to indicate the destination IP Group to where these calls are sent, i.e., to the IP-PBX.
 - 'IP Profile ID': enter "2" to indicate the IP Profile configured for G.723.
4. **Index #3:** routes calls received from the local PSTN network to the IP-PBX:
 - 'Source Trunk Group ID': enter "1" to indicate calls received on the trunk connecting the device to the local PSTN network.
 - 'Dest IP Group ID': select **3** to indicate the destination IP Group to where the calls must be sent, i.e., to the IP-PBX.
5. **Index #4:** routes IP calls received from the IP-PBX to ITSP-A:
 - 'Source IP Group ID': select **3** to indicate received (inbound) calls identified as belonging to the IP Group configured for the IP-PBX.
 - 'Dest Phone Prefix': enter "+81" to indicate calls to Japan (i.e., with prefix +81).
 - 'Source Phone Prefix': enter the asterisk (*) symbol to indicate all sources.
 - 'Dest IP Group ID': select **1** to indicate the destination IP Group to where the calls must be sent, i.e., to ITSP-A.
 - 'IP Profile ID': enter "1" to indicate the IP Profile configured for G.711.
6. **Index #5:** routes IP calls received from the IP-PBX to ITSP-B:
 - 'Source IP Group ID': select **3** to indicate received (inbound) calls identified as belonging to the IP Group configured for the IP-PBX.
 - 'Dest Phone Prefix' and 'Source Phone Prefix': enter the asterisk (*) symbol to indicate all destinations (besides Japan) and all sources respectively.
 - 'Dest IP Group ID': select **2** to indicate the destination IP Group to where the calls must be sent, i.e., to ITSP-A.
 - 'IP Profile ID': enter "1" to indicate the IP Profile configured for G.711.
7. **Index #6:** routes dialed calls (four digits starting with digit 4) from IP-PBX to remote IP-PBX users. The device searches its database for the remote users registered number, and then sends an INVITE to the remote user's IP address (listed in the database):
 - 'Source IP Group ID': select **3** to indicate received (inbound) calls identified as belonging to the IP Group configured for the IP-PBX.
 - 'Dest Phone Prefix': enter the "4xxx#" to indicate all calls dialed from IP-PBX that include four digits and start with the digit 4.
 - 'Dest IP Group ID': select **4** to indicate the destination IP Group to where the calls must be sent, i.e., to remote IP-PBX users.
 - 'IP Profile ID': enter "1" to indicate the IP Profile configured for G.711.

18.10.2.10 Step 10: Configure Destination Phone Number Manipulation

This step defines how to manipulate the destination phone number. The IP-PBX users in our example scenario use a 4-digit extension number. The incoming calls from the ITSP's have different prefixes and different lengths. This manipulation leaves only the four digits of the user's destination number coming from the ITSP's.

➤ **To configure destination phone number manipulation:**

1. Open the Destination Phone Number Manipulation Table for IP -> Tel calls page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** submenu > **Manipulations** submenu > **Dest Number Tel->IP**).

Figure 18-63: Defining Destination Phone Number Manipulation Rules

Index	Source Trunk Group	Source IP Group	Destination Prefix	Source Prefix	Stripped Digits From Left	Stripped Digits From Right
1	-1	-1	+1919	*	0	0
2	-1	-1	0200	*	0	0

Prefix to Add	Suffix to Add	Number of Digits to Leave
		4
		4

2. **Index #1:** defines destination number manipulation of IP calls received from ITSP-A. The phone number of calls received with prefix +1919 (i.e., from ITSP-A) are removed except for the last four digits:
 - 'Destination Prefix': enter the prefix "+1919".
 - 'Source Prefix': enter the asterisk (*) symbol to indicate all sources.
 - 'Number of Digits to Leave': enter "4" to leave only the last four digits.
3. **Index #2:** defines destination number manipulation of IP calls received from ITSP-B. The phone number of calls received with prefix 0200 (i.e., from ITSP-B) are removed except for the last four digits:
 - 'Destination Prefix': enter the prefix "0200".
 - 'Source Prefix': enter the asterisk (*) symbol to indicate all sources.
 - 'Number of Digits to Leave': enter "4" to leave only the last four digits.

19 Stand-Alone Survivability (SAS) Application

This section describes the Stand-Alone Survivability application.

19.1 Overview

The device's Stand-Alone Survivability (SAS) feature ensures telephony communication continuity (survivability) for enterprises using hosted IP services (such as IP Centrex) or IP-PBX in cases of failure of these entities. In case of failure of the IP Centrex, IP-PBX servers (or even WAN connection and access Internet modem), the enterprise typically loses its internal telephony service at any branch, between its offices, and with the external environment. 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.
- Throughout this section, the term *user agent* (UA) refers to the enterprise's LAN phone user (i.e., SIP telephony entities such as IP phones).
- Throughout this section, the term *proxy* or *proxy server* refers to the enterprise's centralized IP Centrex or IP-PBX.
- Throughout this section, the term SAS refers to the SAS application running on the device.

19.1.1 SAS Operating Modes

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

- **Outbound Proxy:** In this mode, SAS receives SIP REGISTER requests from the enterprise's UAs and forwards these requests to the external proxy (i.e., outbound proxy). When a connection with the external proxy fails, SAS enters SAS emergency state and serves as a proxy, by handling internal call routing for the enterprise's UAs - routing calls between UAs and if setup, routing calls between UAs and the PSTN. For more information, see 'SAS Outbound Mode' on page 372.
- **Redundant Proxy:** In this mode, the enterprise's UAs register with the external proxy and establish calls directly through the external proxy, without traversing SAS (or the device per se). Only when connection with the proxy fails, do the UAs register with SAS, serving now as the UAs redundant proxy. SAS then handles the calls between UAs, and between the UAs and the PSTN (if setup). This mode is operational only during SAS in emergency state. This mode can be implemented, for example, for proxies that accept only SIP messages that are sent directly from the UAs. For more information, see 'SAS Redundant Mode' on page 373.



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

19.1.1.1 SAS Outbound Mode

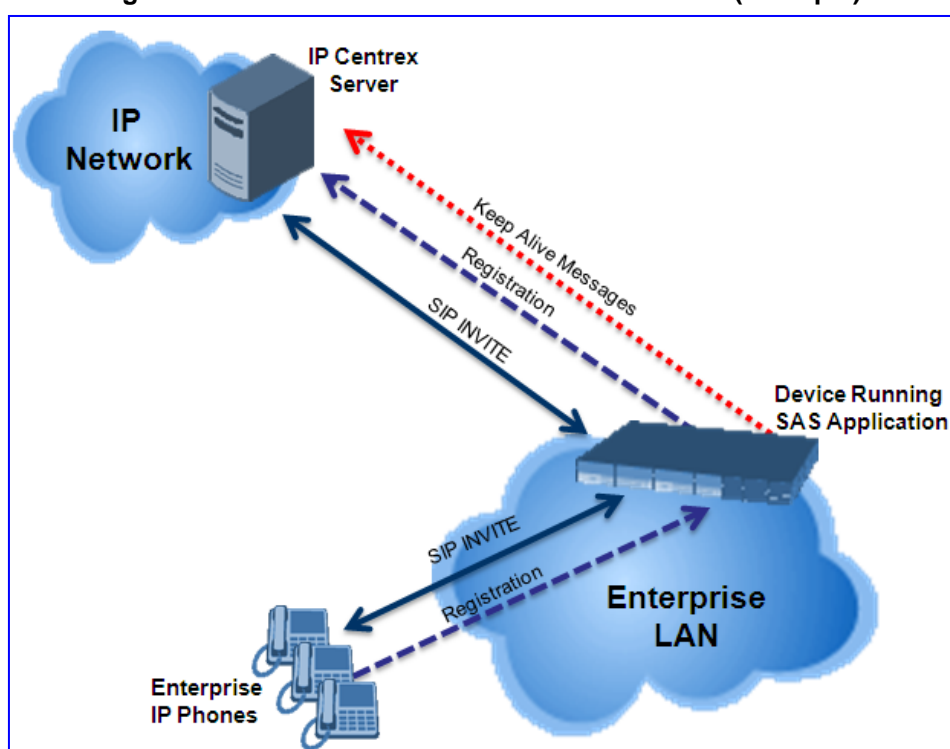
This section describes the SAS outbound mode, which includes the following states:

- Normal state (see 'Normal State' on page 372)
- Emergency state (see 'Emergency State' on page 372)

19.1.1.1.1 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 19-1: SAS Outbound Mode in Normal State (Example)



19.1.1.1.2 Emergency State

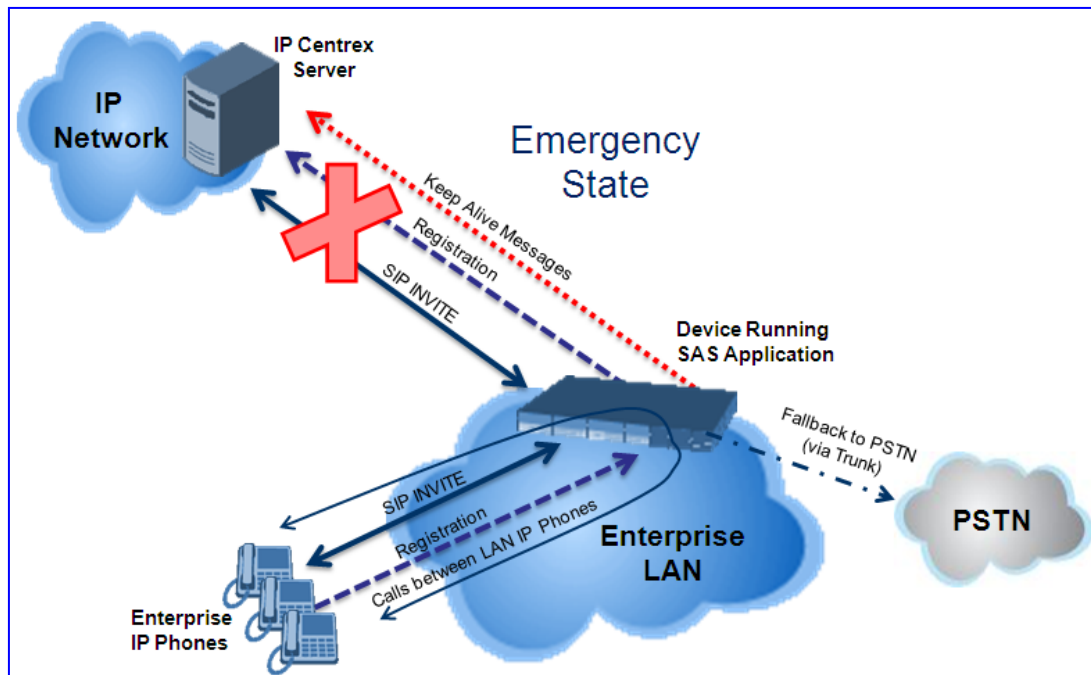
When a connection with the external proxy fails (detected by the device's keep-alive messages), the device enters SAS emergency state. The device serves as a proxy for the UAs, by handling internal call routing of the UAs (within the LAN enterprise).

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 377.

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

Figure 19-2: SAS Outbound Mode in Emergency State (Example)



When emergency state is active, SAS continuously attempts to communicate with the external proxy, using keep-alive SIP OPTIONS. Once connection to the proxy returns, the device exits SAS emergency state and returns to SAS normal state, as explained in 'Exiting Emergency and Returning to Normal State' on page 375.

19.1.1.2 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.

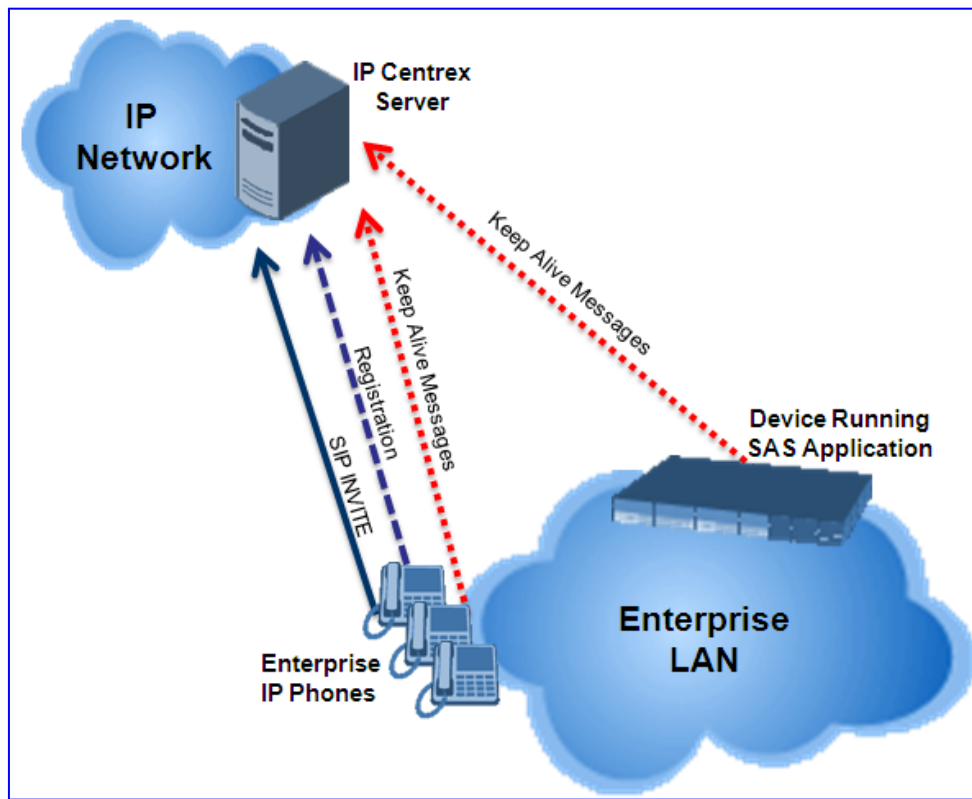


Note: In this SAS deployment, the UAs (e.g., IP phones) must support configuration for primary and secondary proxy servers (i.e., proxy redundancy), as well as homing. Homing allows the UAs to switch back to the primary server from the secondary proxy once the connection to the primary server returns (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.

19.1.1.2.1 Normal State

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

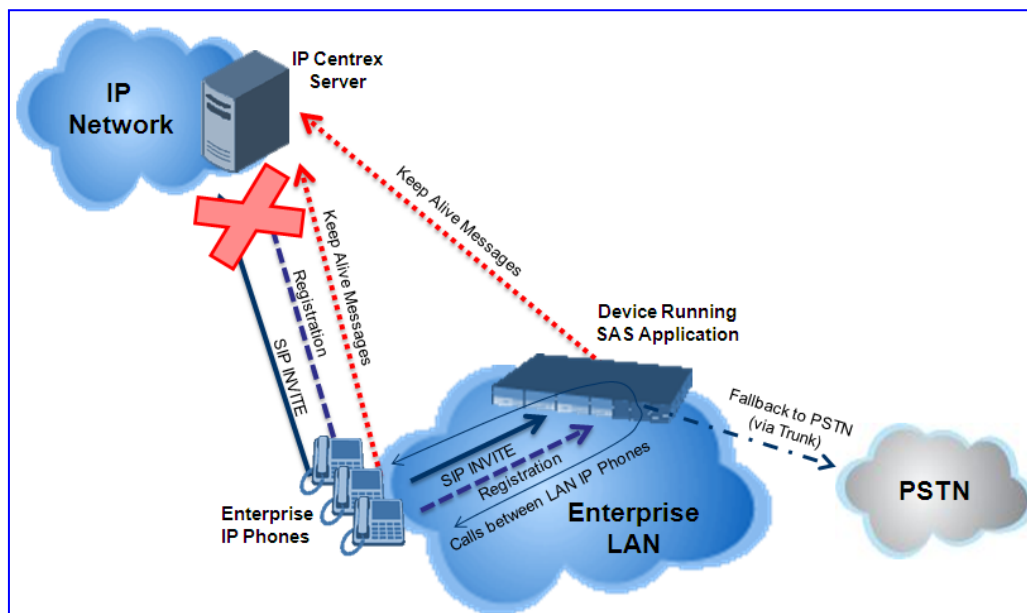
Figure 19-3: SAS Redundant Mode in Normal State (Example)



19.1.1.2.2 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 19-4: SAS Redundant Mode in Emergency State (Example)



19.1.1.2.3 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).

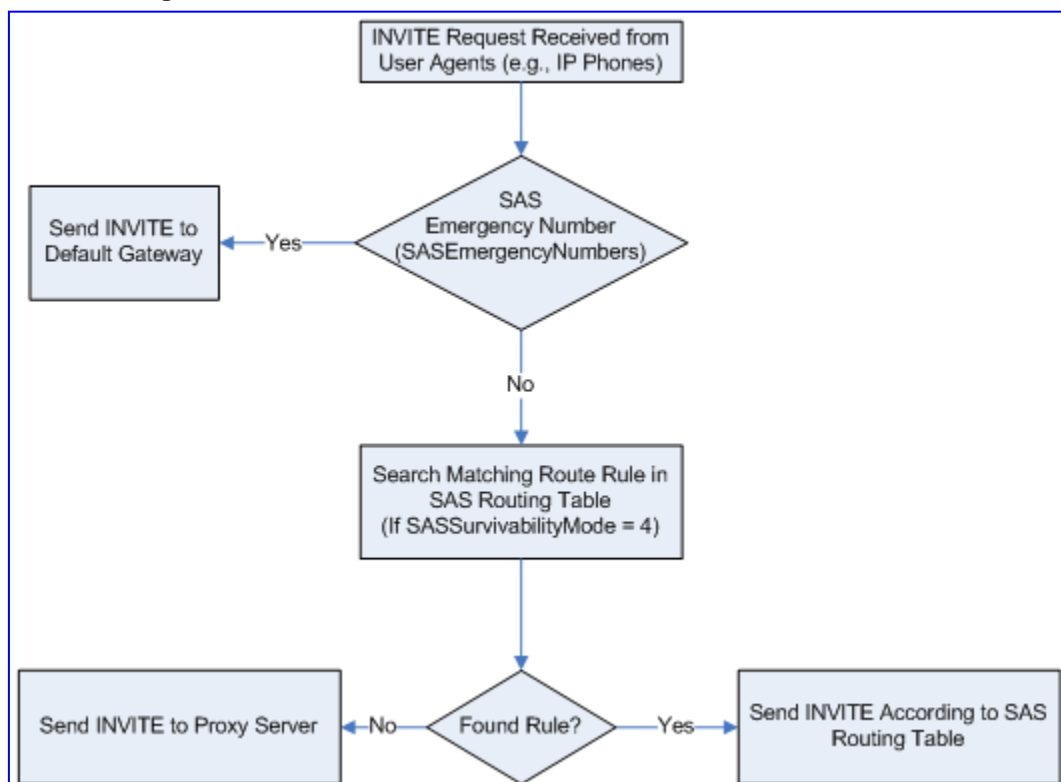
19.1.2 SAS Routing

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

19.1.2.1 SAS Routing in Normal State

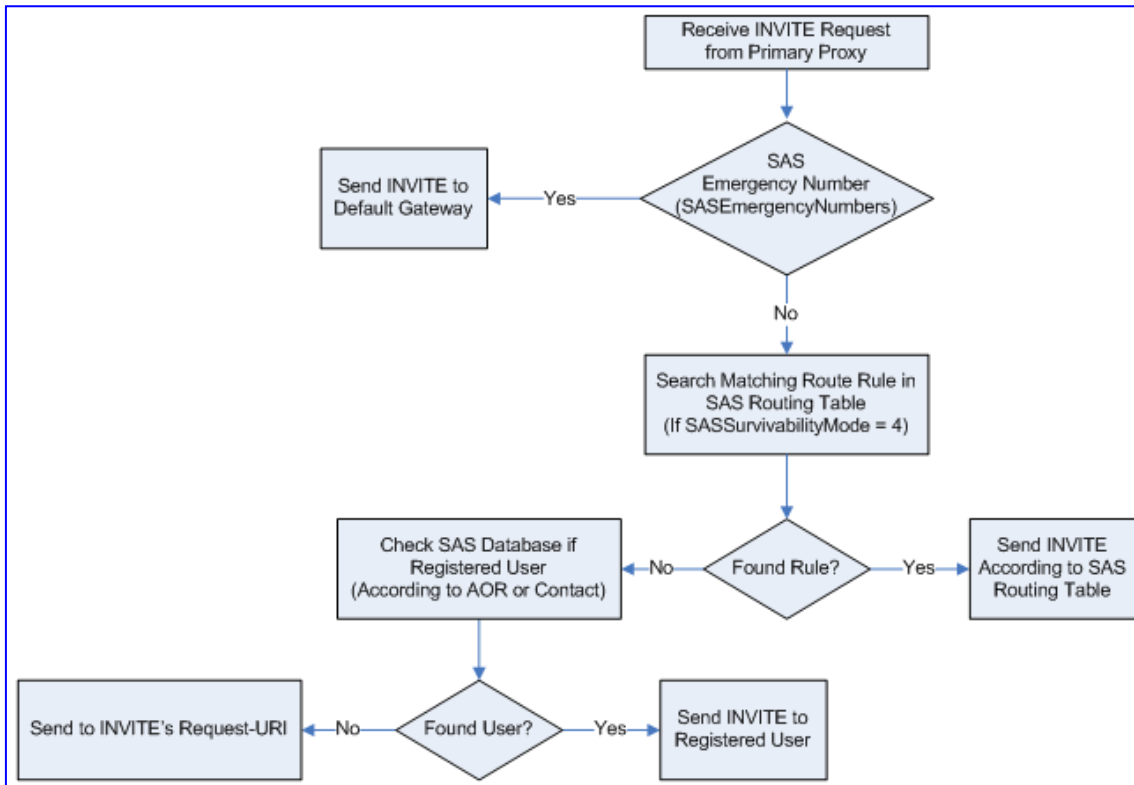
The flowchart below displays the routing logic for SAS in normal state for INVITE messages received from the UAs:

Figure 19-5: Flowchart of INVITE from UA's in SAS Normal State



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

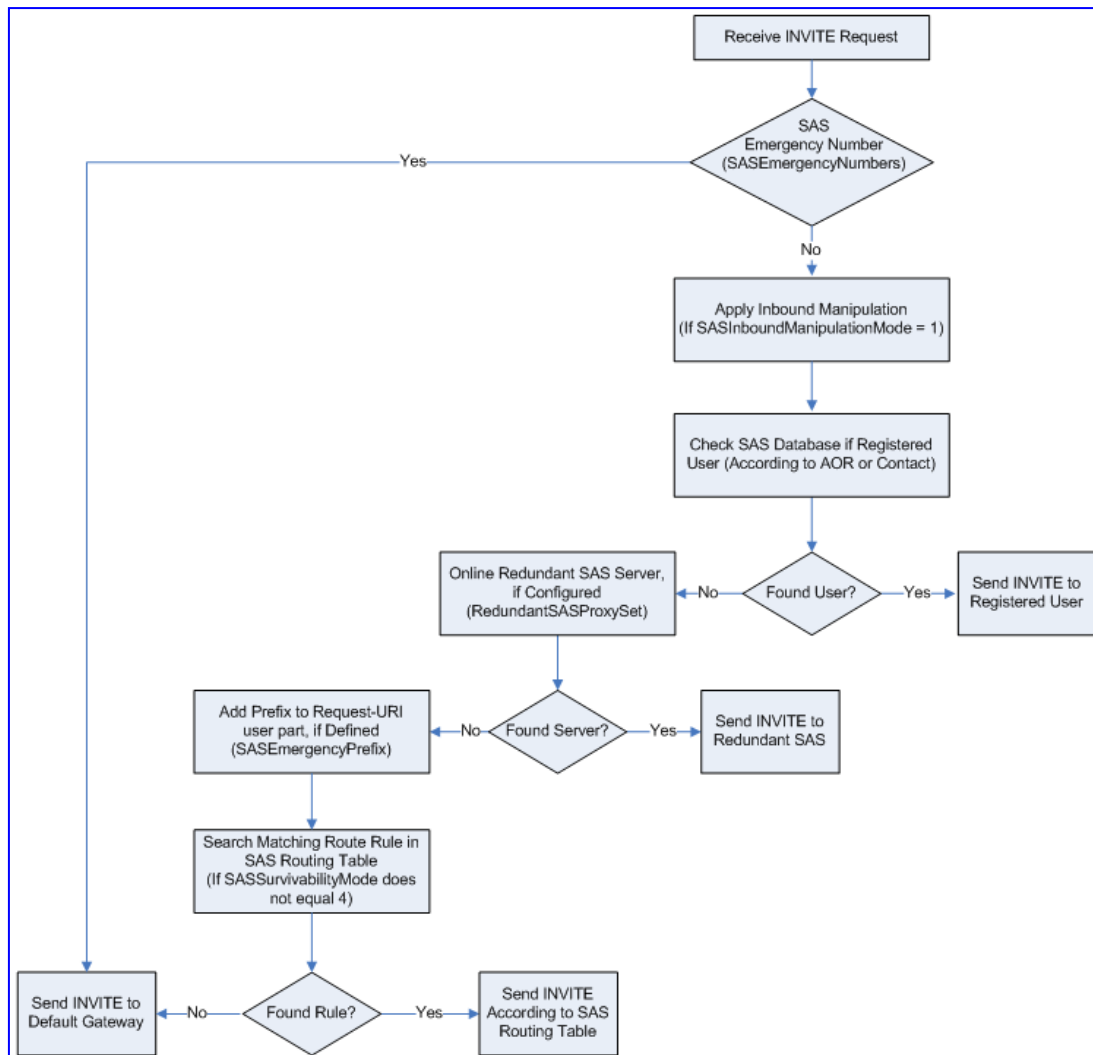
Figure 19-6: Flowchart of INVITE from Primary Proxy in SAS Normal State



19.1.2.2 SAS Routing in Emergency State

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

Figure 19-7: Flowchart for SAS Emergency State



19.2 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 378)
- SAS outbound mode (see 'Configuring SAS Outbound Mode' on page 381)
- SAS redundant mode (see 'Configuring SAS Redundant Mode' on page 382)
- Gateway and SAS applications deployed together (see 'Configuring Gateway Application with SAS' on page 382)
- Optional, advanced SAS features (see 'Advanced SAS Configuration' on page 386)

19.2.1 General SAS Configuration

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

19.2.1.1 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.

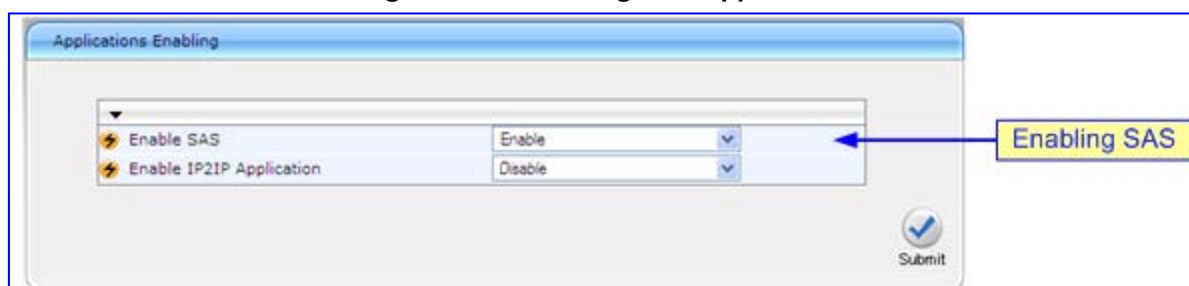


Note: The SAS application is available only if the device is installed with the SAS Software Upgrade Key. If your device is not installed with the SAS feature, contact your AudioCodes representative.

➤ 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 19-8: Enabling 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.

19.2.1.2 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 19-9: Configuring Common Settings

2	SAS Local SIP UDP Port	5080
3	SAS Default Gateway IP	
4	SAS Registration Time	20
2	SAS Local SIP TCP Port	5080
2	SAS Local SIP TLS Port	5081
6	SAS Proxy Set	2
	SAS Emergency Numbers	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
5	SAS Binding Mode	1-User Part Only
	SAS Survivability Mode	Standard
	Enable ENUM	Disable
	Enable Record-Route	Disable
	SAS Block Unregistered Users	Un-Block
	Redundant SAS Proxy Set	-1
	SAS Inbound Manipulation Mode	None

SAS Registration Manipulation	
Remove From Right	Leave From Right
<input type="text" value="0"/>	<input type="text" value="0"/>

SAS Routing
SAS Routing Table

6. In the 'SAS Proxy Set' field, enter the Proxy Set used for SAS. The SAS Proxy Set must be defined only for the following SAS modes:

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

If you define a SAS Proxy Set ID, you must configure the Proxy Set as described in Step 8 below.

7. Click **Submit** to apply your settings.
8. If you defined a SAS Proxy Set ID in Step 6 above, then you must configure the SAS Proxy Set ID:
- Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Networks** > **Proxy Set Table**).
 - From the 'Proxy Set ID' drop-down list, select the required Proxy Set ID.


Notes:

- The selected Proxy Set ID number must be the same as that specified in the 'SAS Proxy Set' field in the 'SAS Configuration' page (see Step 6).
- Do not use Proxy Set ID 0.

- In the 'Proxy Address' field, enter the IP address of the external proxy server.

- b. 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 19-10: Defining UAs' Proxy Server

The screenshot shows the 'Proxy Sets Table' configuration page. At the top, there is a dropdown menu for 'Proxy Set ID' with the value '2'. Below this is a table with two columns: 'Proxy Address' and 'Transport Type'. The table has five rows. The first row contains the IP address '10.15.4.52' and the transport type 'TLS'. The other rows are empty. Below the table, there are several configuration fields. The 'Enable Proxy Keep Alive' field is set to 'Using Options'. Other fields include 'Proxy Keep Alive Time' set to '60' and 'Proxy Load Balancing'. Callouts 'b', 'c', and 'd' are placed on the right side of the interface, pointing to the 'Proxy Set ID' dropdown, the table, and the 'Enable Proxy Keep Alive' dropdown respectively.

- c. Click **Submit** to apply your settings.

19.2.2 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 379.



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**.

19.2.3 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 379.



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**.

19.2.4 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.

19.2.4.1 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 19-11: 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 379).

Figure 19-12: Defining Proxy Server for Gateway Application

	Proxy Address	Transport Type
1	202.10.13.1:5080	UDP
2		
3		
4		
5		

- g. Click **Submit**.

2. Disable use of user=phone in SIP URL:
 - a. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).
 - b. From the 'Use user=phone in SIP URL' drop-down list, select **No**. This instructs the Gateway application not to use *user=phone* in the SIP URL and therefore, REGISTER and INVITE messages use SIP URI. (By default, REGISTER messages are sent with *sip uri* and INVITE messages with *tel uri*.)

Figure 19-13: Disabling user=phone in SIP URL

- c. Click **Submit**.

19.2.4.2 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 19-14: 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 379).
- h. From the 'Proxy Redundancy Mode' drop-down list, select **Homing**.

Figure 19-15: Defining Proxy Servers for Gateway Application

Proxy Sets Table

Proxy Set ID: 0

	Proxy Address	Transport Type
1	202.10.13.1	UDP
2	10.13.4.1	UDP
3		
4		
5		

Enable Proxy Keep Alive: Using Options

Proxy Keep Alive Time: 60

Proxy Load Balancing Method: Disable

Is Proxy Hot Swap: No

Proxy Redundancy Mode: Homing

SRD Index: 1

- i. Click **Submit**.
2. Disable the use of *user=phone* in the SIP URL:
 - a. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).
 - b. From the 'Use user=phone in SIP URL' drop-down list, select **No**. This instructs the Gateway application not to use *user=phone* in SIP URL and therefore, REGISTER and INVITE messages use SIP URI. (By default, REGISTER messages are sent with *sip uri* and INVITE messages with *tel uri*.)

Figure 19-16: Disabling user=phone in SIP URL

SIP General Parameters

Basic Parameter List ▲

SIP Destination Port	5060
Use user=phone in SIP URL	No
Use user=phone in From Header	No
Use Tel URI for Asserted Identity	Disable
Tel to IP No Answer Timeout	180
Enable Remote Party ID	Disable
Add Number Plan and Type to RPI Header	Yes
Enable History-Info Header	Disable
Use Source Number as Display Name	No
Use Display Name as Source Number	No
Enable Contact Restriction	Disable

Submit

- c. Click **Submit**.

19.2.5 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 386)
- Manipulating destination number of incoming SAS INVITE messages (see 'Manipulating Destination Number of Incoming INVITE' on page 387)
- Defining SAS routing rules based on the SAS Routing table (see 'SAS Routing Based on SAS Routing Table' on page 389)
- Blocking unregistered SAS UA's (see 'Blocking Calls from Unregistered SAS Users' on page 392)
- Defining SAS emergency calls (see 'Configuring SAS Emergency Calls' on page 392)
- Adding SIP Record-Route header to INVITE messages (see 'Adding SIP Record-Route Header to SIP INVITE' on page 394)
- Replacing SIP Contact header (see 'Replacing Contact Header for SIP Messages' on page 395)

19.2.5.1 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 19-17: Manipulating User Part in Incoming REGISTER

SAS Local SIP UDP Port	5060
SAS Default Gateway IP	10.0.0.2:5080
SAS Registration Time	20
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	0
SAS Emergency Numbers	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
SAS Binding Mode	0-URI
SAS Survivability Mode	Always Emergency
Enable ENUM	Disable
Enable Record-Route	Disable
SAS Block Unregistered Users	Un-Block
Redundant SAS Proxy Set	-1
SAS Inbound Manipulation Mode	None

SAS Registration Manipulation	
Remove From Right	Leave From Right
<input type="text" value="0"/>	<input type="text" value="4"/>

SAS Routing
SAS Routing Table

3. Click **Submit**.

19.2.5.2 Manipulating Destination Number of Incoming INVITE

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

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

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

➤ **To manipulate destination number in SAS emergency state:**

1. Enable inbound manipulation for SAS in Emergency mode:
 - a. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
 - b. From the 'SAS Inbound Manipulation Mode' (*SASInboundManipulationMode*) drop-down list, select **Emergency Only**.
 - c. Click **Submit** to apply your changes.
2. Configure the manipulation rule:
 - a. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
 - b. Open the IP to IP Inbound Manipulation page, by clicking the **IP to IP Inbound Manipulation Table** button.

Figure 19-18: Manipulating INVITE Destination Number

Manipulated URI	Manipulation Purpose	Source IP Group	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	Request Type	Remove From Left	Remove From Right	Leave From Right	Prefix to Add
Destination	Normal	-1			700xxxx		INVITE	3	0	255	55215555

The figure above displays a manipulation rule for the example scenario described above whereby the destination number "7001234" is changed to "552155551234":

- ◆ 'Manipulated URI' field: **Destination**
 - ◆ 'Destination Username Prefix' field: "700xxxx"
 - ◆ 'Request Type' field: **INVITE**
 - ◆ 'Remove From Left' field: "3"
 - ◆ 'Prefix to Add' field: "55215555"
- c. Click **Apply** to save your changes.



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**.
- This table is currently located under the SBC menu.

19.2.5.3 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 more information on the SAS Routing table, see 'Configuring IP2IP Routing Table (SAS)' on page 389.

19.2.5.3.1 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 'Configuration Parameters Reference' on page 529).

➤ To configure the IP2IP Routing table for SAS:


1. In the SAS Configuration page, click the **SAS Routing Table**  button; the IP2IP Routing Table page appears.

Figure 19-19: IP2IP Routing Page

Index	Source IP Group ID	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	
1		*	*	*	*	
		RequestType	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Address
		All	IP Group			
			Destination Port	Destination Transport Type	Alternative Route Options	
			0		Route Row	

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 470.



Note: The following parameters are not applicable to SAS and should be ignored: Destination IP Group ID, and Alternative Route Options.

Table 19-1: 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 767.
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 "*".
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 "*".
RequestType [IP2IPRouting_RequestType]	The SIP dialog request type of the incoming SIP dialog. <ul style="list-style-type: none"> ▪ [0] All (default) ▪ [1] INVITE ▪ [2] REGISTER ▪ [3] SUBSCRIBE ▪ [4] INVITE and REGISTER ▪ [5] INVITE and SUBSCRIBE
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. <ul style="list-style-type: none"> ▪ [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

Parameter	Description
	<p>overridden and these fields take precedence.</p> <ul style="list-style-type: none"> ▪ [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 Address [IP2IPRouting_DestAddress]	<p>The destination IP address (or domain name, e.g., domain.com) to where the call is sent.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 124).
Destination Port [IP2IPRouting_DestPort]	<p>The destination port to where the call is sent.</p>
Destination Transport Type [IP2IPRouting_DestTransportType]	<p>The transport layer type for sending the call:</p> <ul style="list-style-type: none"> ▪ [-1] Not Configured (default) ▪ [0] UDP ▪ [1] TCP ▪ [2] TLS <p>Note: When this parameter is set to -1, the transport type is determined by the parameter SIPTransportType.</p>

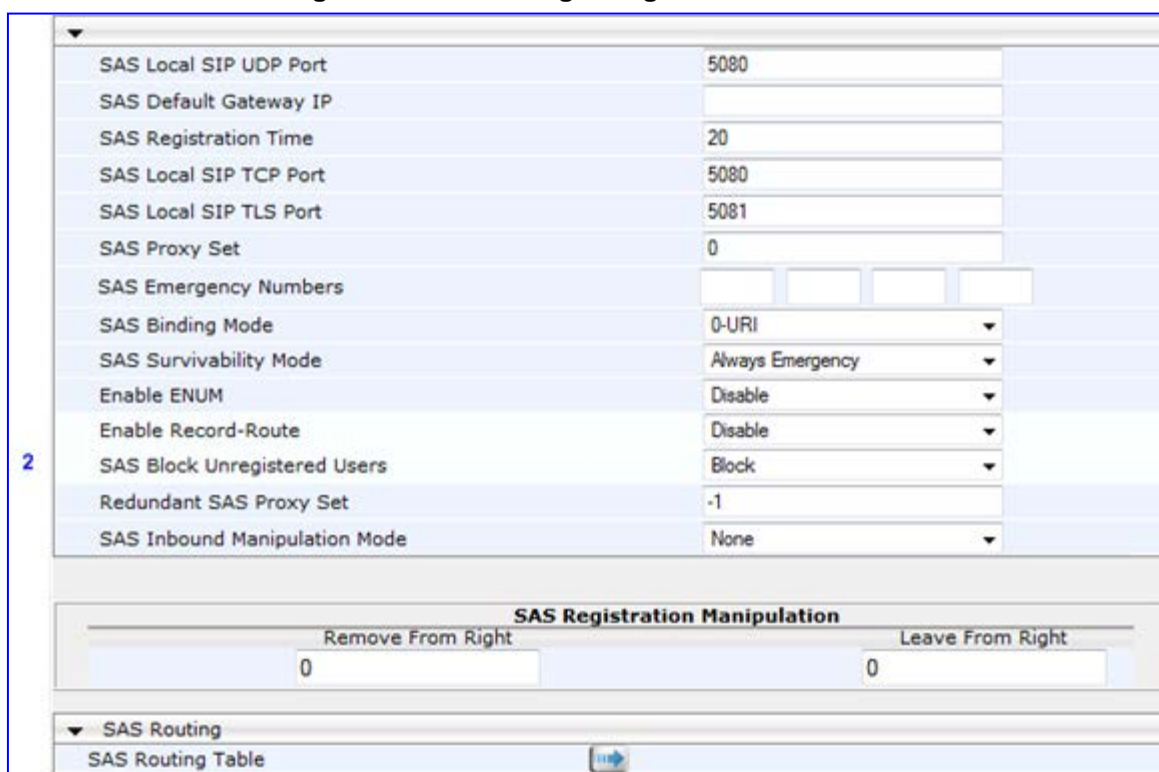
19.2.5.4 Blocking Calls from Unregistered SAS Users

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**, as shown below:

Figure 19-20: Blocking Unregistered SAS Users



The screenshot shows the SAS Configuration page with the following settings:

SAS Local SIP UDP Port	5080
SAS Default Gateway IP	
SAS Registration Time	20
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	0
SAS Emergency Numbers	
SAS Binding Mode	0-URI
SAS Survivability Mode	Always Emergency
Enable ENUM	Disable
Enable Record-Route	Disable
SAS Block Unregistered Users	Block
Redundant SAS Proxy Set	-1
SAS Inbound Manipulation Mode	None

Below the main configuration area is the 'SAS Registration Manipulation' section with two input fields: 'Remove From Right' (value: 0) and 'Leave From Right' (value: 0). At the bottom, there is a 'SAS Routing' section with a 'SAS Routing Table' button.

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

19.2.5.5 Configuring SAS Emergency Calls

You can configure SAS to route emergency calls (such as 911 in North America) directly to the PSTN (through its FXO interface or E1/T1 trunk). 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 377). 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 19-21: Configuring SAS Emergency Numbers

	SAS Local SIP UDP Port	5080
2	SAS Default Gateway IP	10.13.4.12
	SAS Registration Time	20
	SAS Local SIP TCP Port	5080
	SAS Local SIP TLS Port	5081
	SAS Proxy Set	0
3	SAS Emergency Numbers	911
	SAS Binding Mode	1-User Part Only
	SAS Survivability Mode	Always Emergency
	Enable ENUM	Disable
	Enable Record-Route	Disable
	SAS Block Unregistered Users	Block
	Redundant SAS Proxy Set	-1
	SAS Inbound Manipulation Mode	None
SAS Registration Manipulation		
	Remove From Right	Leave From Right
	0	0
SAS Routing SAS Routing Table		

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

19.2.5.6 Adding SIP Record-Route Header to SIP INVITE

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

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



Notes:

- This feature is applicable only to SAS outbound mode.
- This feature can also be enabled using the `SASEnableRecordRoute ini` file parameter.

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

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the 'Enable Record-Route' drop-down list, select **Enable**.

Figure 19-22: Enabling SIP Record-Route Header

SAS Local SIP UDP Port	5080
SAS Default Gateway IP	10.13.4.12
SAS Registration Time	20
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	0
SAS Emergency Numbers	911
SAS Binding Mode	1-User Part Only
SAS Survivability Mode	Always Emergency
Enable ENUM	Disable
2 Enable Record-Route	Enable
SAS Block Unregistered Users	Block
Redundant SAS Proxy Set	-1
SAS Inbound Manipulation Mode	None

SAS Registration Manipulation

Remove From Right	Leave From Right
0	0

▼ SAS Routing

SAS Routing Table

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

19.2.5.7 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.

**Notes:**

- 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.

19.3 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 508. The maximum number of users that can be registered in the database is 600.



Note: Despite the maximum number of SAS users, you can increase this capacity by implementing the SAS Cascading feature, as described in 'SAS Cascading' on page 396.

19.4 SAS Cascading

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

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

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

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

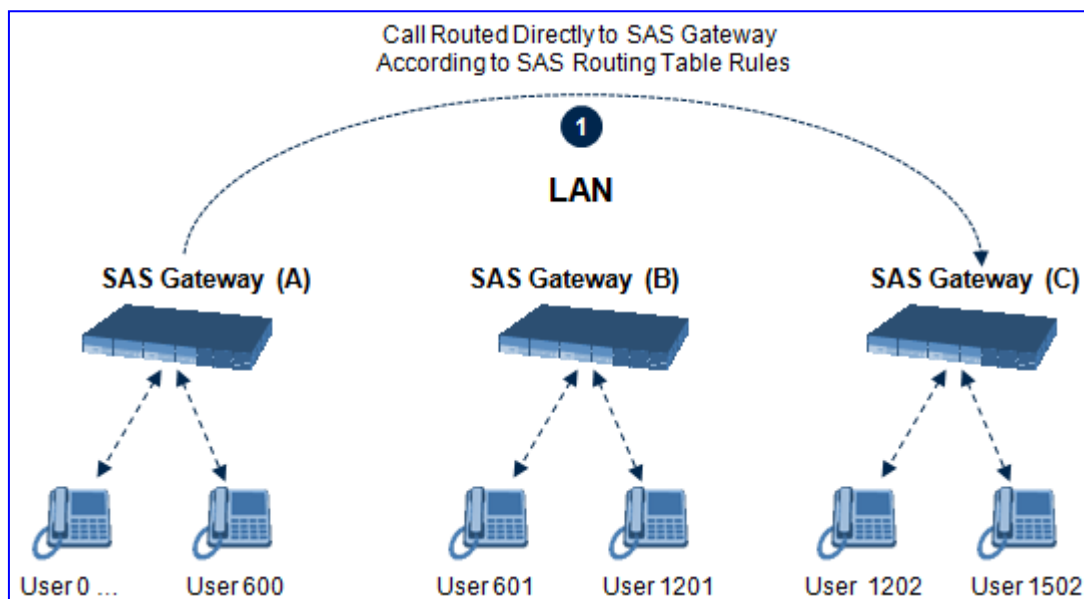
The following is an example of a SAS Cascading deployment of users with unique phone extension numbers:

- users registered to the first SAS gateway start with extension number "40"
- users registered to the second SAS gateway start with extension number "20"
- users registered to the third SAS gateway start with extension number "30"

The SAS Routing table rules for SAS Cascading are created using the destination (called) extension number prefix (e.g., "30") and the destination IP address of the SAS gateway to which the called user is registered. Such SAS routing rules must be configured at each SAS gateway to allow routing between the SAS users. The routing logic for SAS Cascading is similar to SAS routing in Emergency state (see the flowchart in 'SAS Routing in Emergency State' on page 377). For a description on the SAS Routing table, see 'SAS Routing Based on SAS Routing Table' on page 389.

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

Figure 19-23: SAS Cascading Using SAS Routing Table - Example

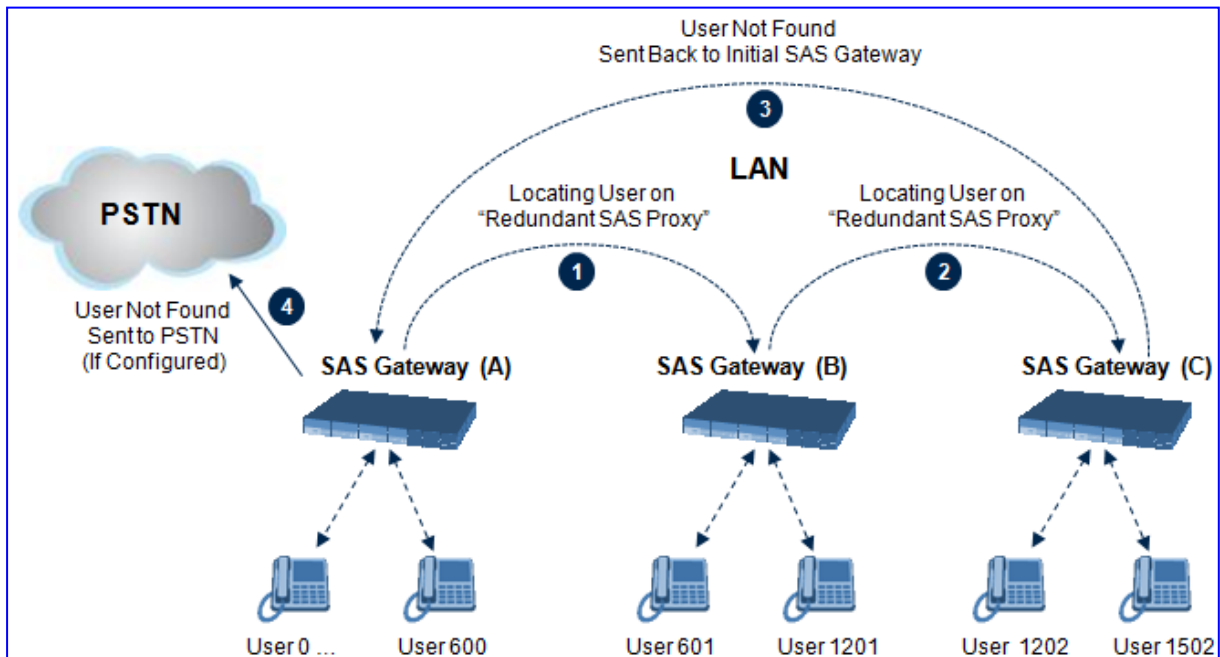


- SAS Redundancy mode:** If users cannot be distinguished (i.e., associated to a specific SAS gateway), then the SAS Redundancy feature is used to configure SAS Cascading. This mode routes the call in a loop fashion, from one SAS gateway to the next, until the user is located. Each SAS gateway serves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

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

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

Figure 19-24: SAS Cascading Using SAS Redundancy Mode - Example



20 Configuring the IP Media Parameters

The IP Media Settings page allows you to configure IP media parameters. For a description of these parameters, see 'Configuration Parameters Reference' on page 529.



Note: This page is applicable only to Mediant 1000. This page appears only if your device is installed with the relevant Software Upgrade Key (see 'Loading Software Upgrade Key' on page 485).

➤ **To configure the IP media parameters:**

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

Figure 20-1: IP Media Settings Page

Number of Media Channels	<input type="text" value="0"/>
Voice Streaming	<input type="text" value="Disable"/>
NetAnn Announcement ID	<input type="text" value="annc"/>
MSCML ID	<input type="text" value="ivr"/>
Transcoding ID	<input type="text" value="trans"/>
▼ Conference	
Conference ID	<input type="text" value="conf"/>
Beep on Conference	<input type="text" value="Enable"/>
Enable Conference DTMF Clamping	<input type="text" value="Enable"/>
Enable Conference DTMF Reporting	<input type="text" value="Disable"/>

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see 'Saving Configuration' on page 470.

20.1 Overview

This section provides information on the device's media server capabilities:

- Multi-party conferencing (see 'Conference Server' on page 400)
- Playing and recording Announcements (see 'Announcement Server' on page 414)
- IP-to-IP Transcoding (see 'IP-to-IP Transcoding' on page 462)
- Voice XML Interpreter (see Voice XML Interpreter on page 438)



Note: This section is applicable only to Mediant 1000.

The device conference, transcoding, announcement and media server applications can be used separately, each on a different platform, or all on the same device. The SIP URI name in the INVITE message is used to identify the resource (media server, conference or announcement) to which the SIP session is addressed.

The number of DSP channels that are allocated for IP conferences, transcoding and IP announcements is determined by the parameter MediaChannels. Other DSP channels can be used for PSTN media server.

The device's SIP implementation is based on the decomposition model described in the following IETF Internet-Drafts:

- "A Multi-party Application Framework for SIP" (draft-ietf-sipping-cc-framework-06)
- "Models for Multi Party Conferencing in SIP" (draft-ietf-sipping-conferencing-framework-05)
- "A Framework for Conferencing with the Session Initiation Protocol (SIP)" (RFC 4353)
- "Basic Network Media Services with SIP" (RFC 4240)
- "Media Server Control Markup Language (MSCML) and Protocol" (draft-vandyke-mscml-06)



Note: To use the device's advanced Announcement capabilities, it's essential that the *ini* file parameter AMSProfile be set to 1.

20.1.1 Conference Server

The device supports dial-in, multi-party conferencing. In conference applications, the device functions as a centralized conference bridge. In ad-hoc or prearranged conferences, users 'invite' the conference bridge. The conference bridge mixes the media and sends it to all participants.

The device supports the following interfaces for conferencing:

- Simple, according to NetAnn (see 'Simple Conferencing (NetAnn)' on page 401)
- Advanced, according to MSCML (see 'Advanced Conferencing (MSCML)' on page 403)

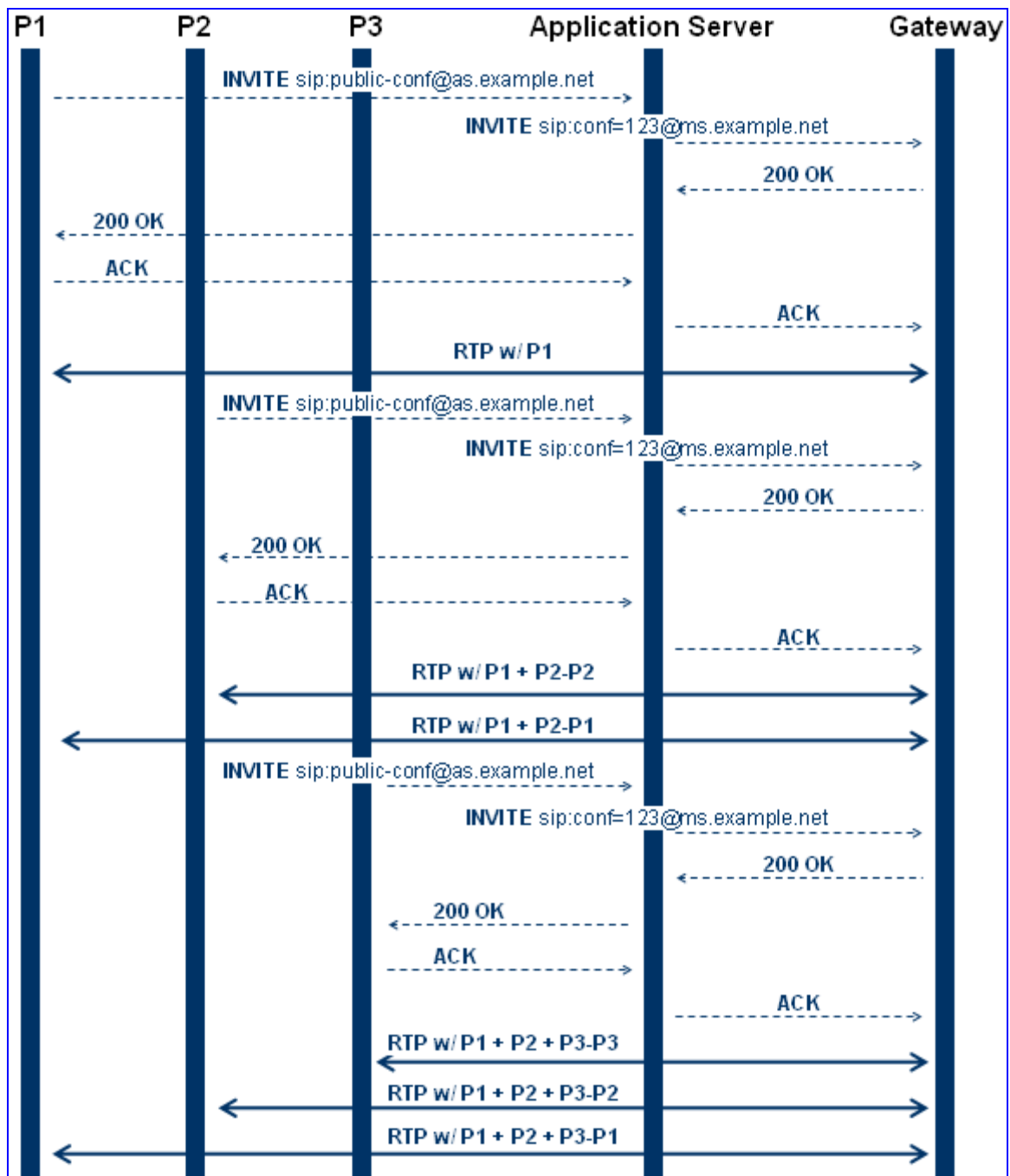


Note: The conference application is a special order option.

20.1.1.1 Simple Conferencing (NetAnn)

20.1.1.1.1 SIP Call Flow

A SIP call flow for simple conferencing is shown below:



20.1.1.1.2 Creating a Conference

The device creates a conference call when the first user joins the conference. To create a conference, the Application Server sends a regular SIP INVITE message to the device. The User Part of that Request-URI includes both the Conference Service Identifier

(indicating that the requested Media Service is a Conference) and a Unique Conference Identifier (identifying a specific instance of a conference).

```
INVITE sip: conf100@audiocodes.com SIP/2.0
```

By default, a request to create a conference reserves three resources on the device. It is possible to reserve a larger number of resources in advance by adding the number of required participants to the User Part of the Request-URI. For example, '6conf100' reserves six resources for the duration of the conference. If the device can allocate the requested number of resources, it responds with a 200 OK.

The Conference Service Identifier can be set using the 'Conference ID' parameter (ConferenceID) in the IP Media Settings page (see 'Configuring the IP Media Parameters' on page 399). By default, it is set to 'conf'.

20.1.1.1.3 Joining a Conference

To join an existing conference, the Application Server sends a SIP INVITE message with the same Request-URI as the one that created the conference. Each conference participant can use a different coder negotiated with the device using usual SIP negotiation.

If more than the initially requested number of participants try to join the conference (i.e., four resources were reserved and a fifth INVITE is received) and the device has an available resource, the request is granted.

If an INVITE to join an existing conference is received with a request to reserve a larger number of participants than initially requested, it is granted if the device has available resources. A request for a smaller number of participants is not granted as this may create a situation where existing legs would need to be disconnected.

The maximal number of participants in a single conference is 60. The maximal number of participants that actually participate in the mix at a given time is three (the loudest legs).

The Application Server can place a participant on Hold/Un-hold by sending the appropriate SIP Re-INVITE on that participant dialog.

20.1.1.1.4 Terminating a Conference

The device never disconnects an existing conference leg. If a BYE is received on an existing leg, it is disconnected, but the resource is still saved if the same leg (or a different one) wants to re-join the conference. This logic occurs only for the initial number of reserved legs.

For example:

1. INVITE reserves three legs.
2. A, B, and C join the conference.
3. A disconnects.
4. A joins (guaranteed).
5. D joins.
6. A disconnects.
7. A joins (not guaranteed).

Sending a BYE request to the device terminates the participant's SIP session and removes it from the conference. The final BYE from the last participant ends the conference and releases all conference resources.

20.1.1.1.5 PSTN Participants

Adding PSTN participants is done by performing a loopback from the IP side (the device's IP address is configured in the Outbound IP Routing Table). If the destination phone number in the incoming call from the PSTN is equal to the Conference Service Identifier and Unique Conference Identifier, the participant joins the conference.

A PSTN participant uses two DSP channels (caused by the IP loopback).

20.1.1.2 Advanced Conferencing (MSCML)

20.1.1.2.1 Creating a Conference

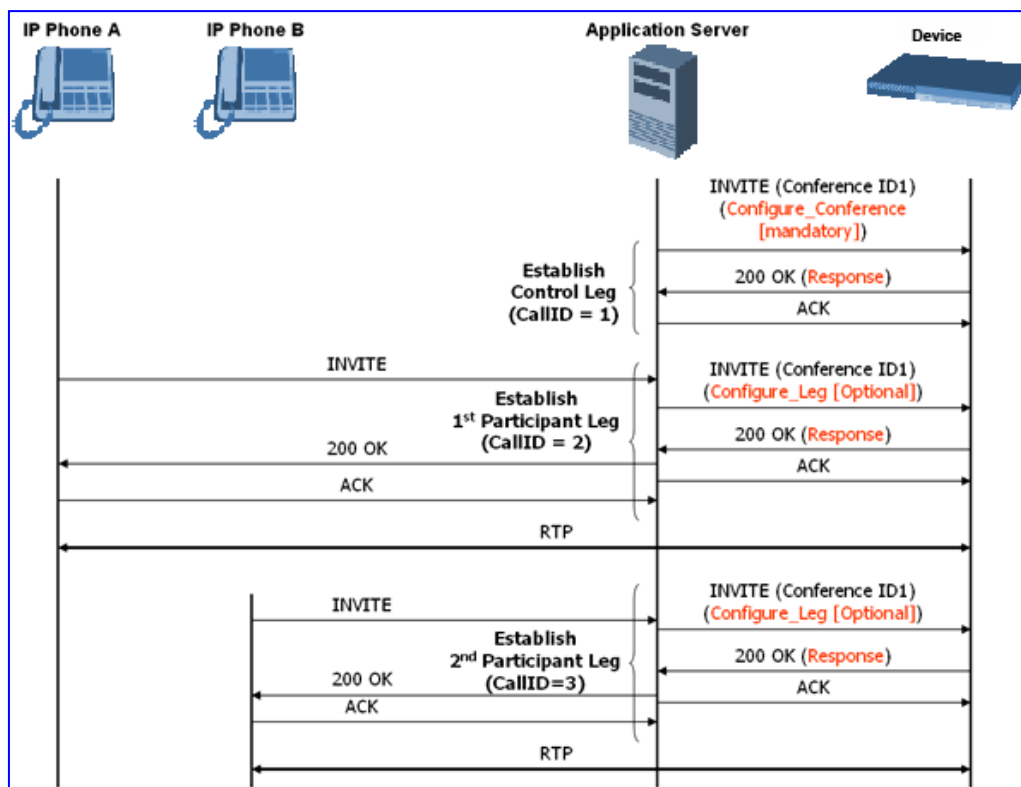
The device creates a conference call when the first INVITE is received from the Application Server (same as NetAnn). The Unique Conference Identifier is used to join participants to the same conference. This first INVITE must include a `<configure_conference>` MSCML request body. If this body is not included, a simple conference is established. This first leg is the Control Leg, which is different from a regular Participant Leg. The Control Leg is used to perform operations for the whole conference.

The MSCML response to the first INVITE is sent in the 200 OK SIP response. If no error occurs, the response is:

```
<response request="configure_conference" code="200" text="OK"/>
```

The `<configure_conference>` can include the following attributes:

- **Id:** identification number of the MSCML request. This is used to correlate between MSCML requests and responses.
- **Reservedtalkers:** defines the maximum number of talker legs. As the device does not support "listener only" legs, this actually sets the maximum number of participants in the conference. The device reserves this number of participants for the entire duration of the conference. If a participant leg decides to leave the conference by issuing a BYE, the resource is not freed, thereby allowing that same leg (or a new one) to join at any stage.
- **Reserveconfmedia:** determines if Media Services such as Play or Record can be applied to the conference. If set to Yes, the device reserves the necessary amount of resources to play an announcement to the whole conference or record the whole conference. The Application Server can change the value of `reserveconfmedia` during an existing conference. By default, `reserveconfmedia` is set to Yes.



20.1.1.2.2 Joining a Conference

To join an existing conference, the Application Server sends a SIP INVITE message with the same Request-URI as the one that created the conference. The INVITE message may include a `<configure_leg>` MSCML request body. If not included, defaults are used for that leg attributes.

The `<configure_leg>` can include the following attributes:

- **Id:** identification number of the MSCML request. This is used to correlate between MSCML requests and responses.
- **Type:** Talker / Listener. If set to Listener, the incoming RTP from that leg does not participate in the conference mix. The default is Talker.
- **Mixmode:**
 - Full: RTP from this leg participates in the mix (default).
 - Mute: RTP from this leg is not participating in the mix.
 - Private: RTP from this leg can only hear participants within a conference team (`<teammate>`) to which it belongs (see below).

The `<configure_team>` element enables clients to create personalized mixes for scenarios where the standard mixmode settings do not provide sufficient control. The `<configure_team>` element is a child of `<configure_leg>`. The `<configure_team>` element, containing one or more `<teammate>` elements, specifies those participants that should be present in this participant's personalized mix. The `<configure_team>` element supports several commands: set, add, remove, and query.

The participants are identified in the `<teammate>` elements by their IDs that are assigned in their `<configure_leg>` element. The team configuration is implicitly symmetric, i.e. if participant A defines participant B as its team member, implicitly participant B defines participant A as its team member.

A "coaching" example:

Table 20-1: MSCML Conferencing with Personalized Mixes

Participant	ID	Team Members	Mixmode	Hears
Supervisor	"supervisor"	Agent	Private	Customer and Agent
Agent	"agent"	Supervisor	Full	Customer and Supervisor
Customer	"customer"		Full	Agent

This scenario is established as follows:

1. Conference is created on the control leg with <configure_conference>.

2. Coach leg joins and issues:

```
<configure_leg id="supervisor" mixmode="private"/>
```

3. Agent leg joins and issues:

```
<configure_leg id="agent">
  <configure_team action="set">
    <teammate id="supervisor"/>
  </configure_team>
</configure_leg>
```

4. Customer joins and issues:

```
<configure_leg id="customer"/>
```

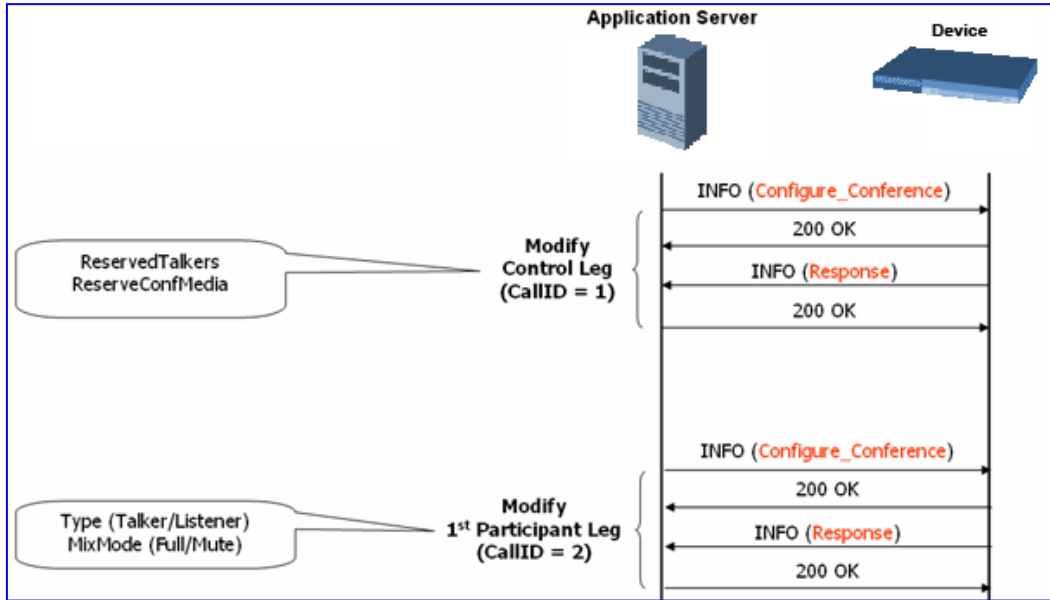
20.1.1.2.3 Modifying a Conference

To modify an existing conference, INFO messages are used. Each INFO message carries an MSCML request. The MSCML response is included in an INFO message back from the device to the Application Server. It is possible to modify an entire conference (by issuing requests on the Control Leg) or only a certain participant (by issuing requests on that specific leg).

To modify the entire conference, a <configure_conference> MSCML request body is sent in an INFO message on the Control Leg SIP dialog. Using this request, the Application Server can modify the following attributes:

- **Reservetalkers:** If the Application Server sets a number that is lower than the initial number requested in the INVITE, then the request is not granted. If the number is higher than the initial number, the device sends a success response in the response INFO.
- **Reserveconfmedia:** If the necessary resources for applying Media Services on the entire conference were reserved in advance, then by setting reserveconfmedia to Yes, it is reserved. If set to No, the device can free the resource.

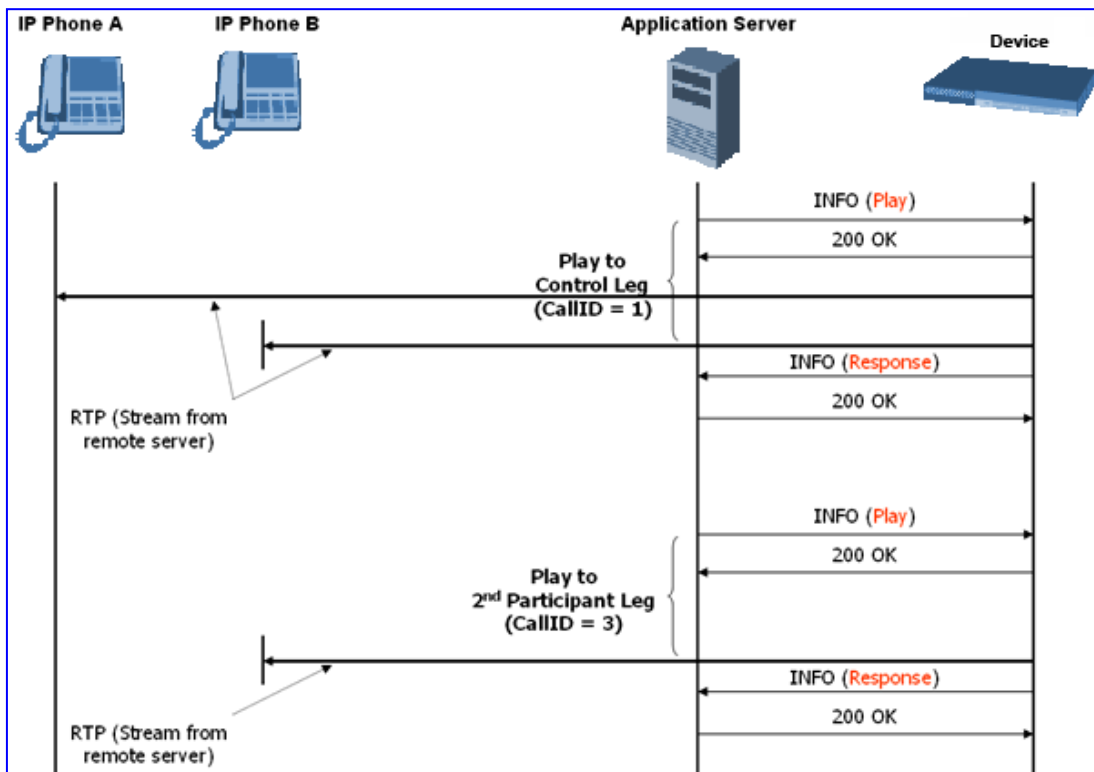
To modify a certain Participant Leg, a <configure_leg> MSCML request body is sent in an INFO message on that leg SIP dialog. Using this request, the Application Server can modify any of the attributes defined for the <configure_leg> request.



20.1.1.2.4 Applying Media Services on a Conference

The Application Server can issue a Media Service request (<play>, <playcollect>, or <playrecord>) on either the Control Leg or a specific Participant Leg. For a Participant Leg, all three requests are applicable. For the Control Leg, the <playcollect> is not applicable as there is no way to collect digits from the whole conference.

When issuing a Media Service on the Control Leg, it affects all Participant Legs in the conference, e.g., play an announcement. When issuing a Media Service on a Participant Leg, it affects the specific leg only.



20.1.1.2.5 Active Speaker Notification

After an advanced conference is established, the Application Server can subscribe to the device to receive notifications of the current set of active speakers in a conference at any given moment. This feature is referred to as *Active Speaker Notification (ASN)* and is designed according to the MSCML standard. Notifications provide information on the number of active participants and their details.

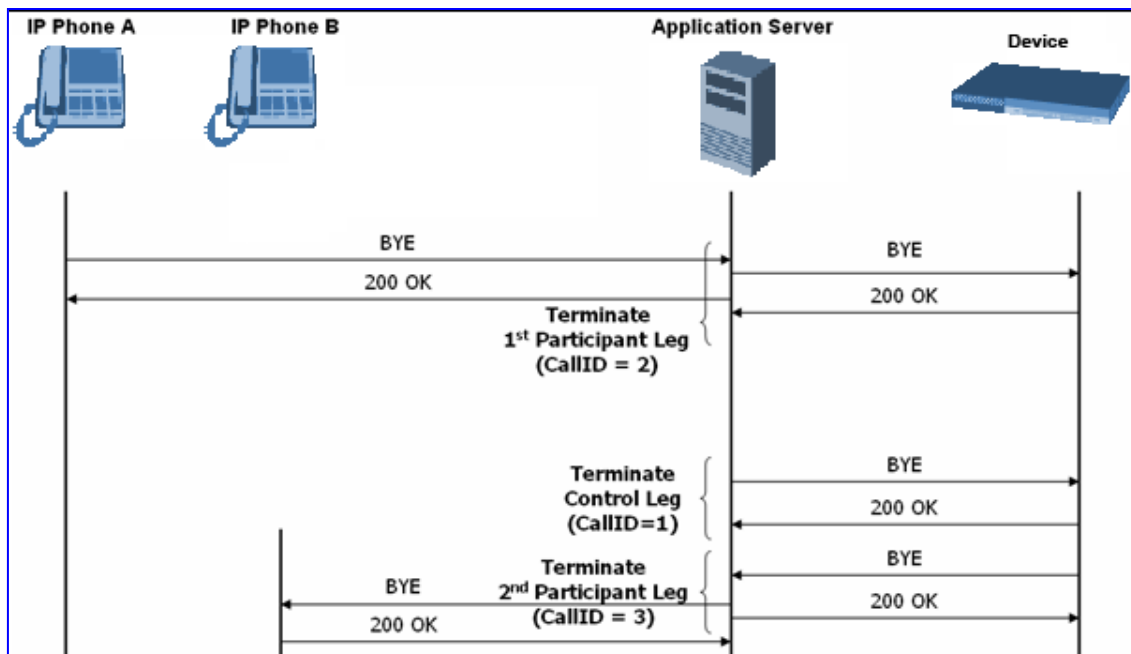
The notifications are sent unsolicited at specific intervals requested by the application and only when a change in the number of active conference speakers occurs. If a change in the speakers list occurs, the server issues an INVITE to the specific SIP UA, and then transfers the call to the UA.

Event notifications are sent in SIP INFO messages, as shown in the example below of XML Response Generated for ASN:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
<notification>
<conference uniqueID="3331" numtalkers="1">
<activetalkers>
<talker callID="9814266171512000193619@10.8.27.118"/>
</activetalkers>
</conference>
</notification>
</MediaServerControl>
```

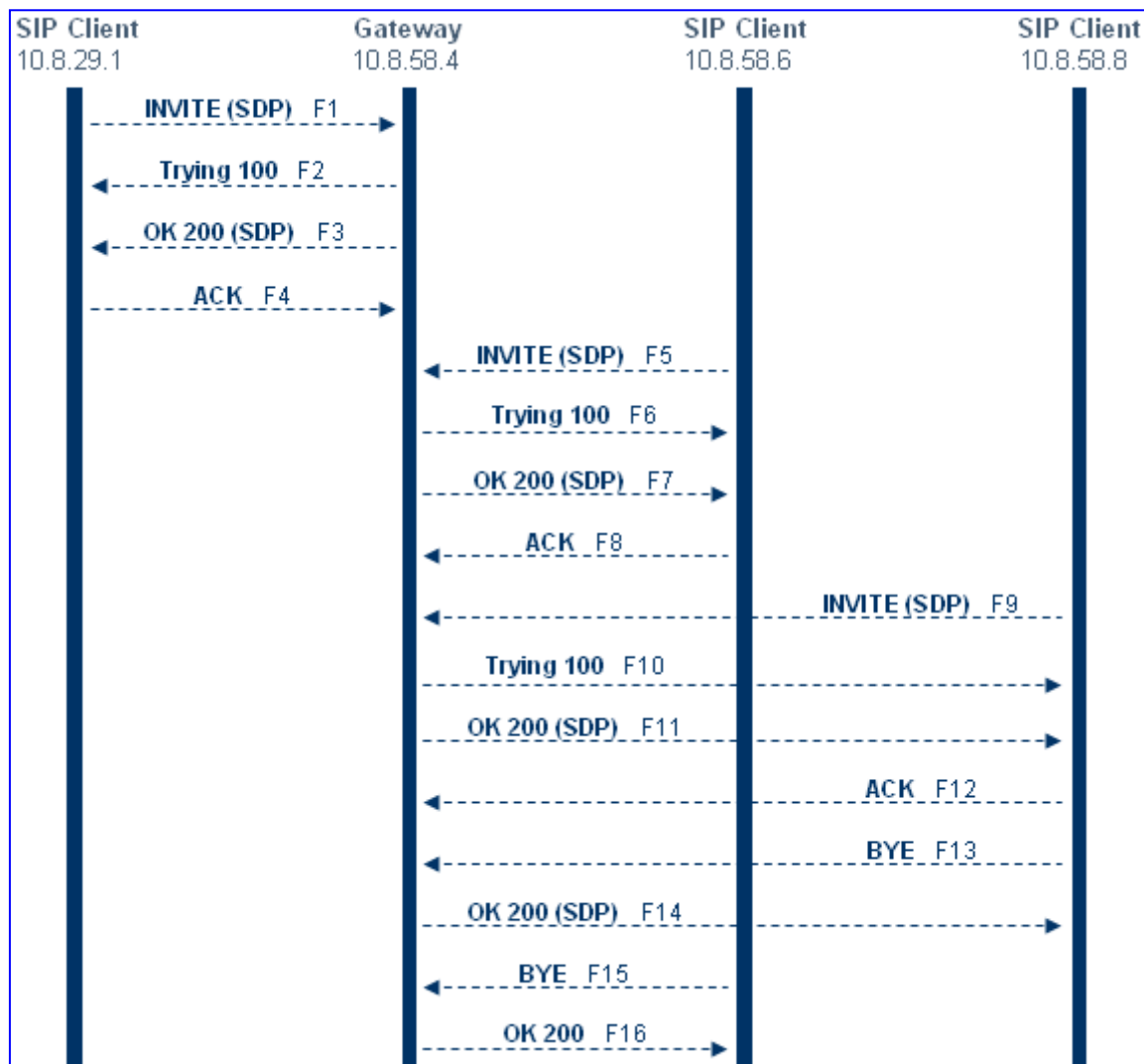
20.1.1.2.6 Terminating a Conference

To remove a leg from a conference, the Application Server issues a SIP BYE request on the selected dialog representing the conference leg. The Application Server can terminate all legs in a conference by issuing a SIP BYE request on the Control Leg. If one or more participants are still in the conference when the device receives a SIP BYE request on the Control Leg, the device issues SIP BYE requests on all of the remaining conference legs to ensure a clean up of the legs.



20.1.1.3 Conference Call Flow Example

The call flow, shown in the following figure, describes SIP messages exchanged between the device (10.8.58.4) and three conference participants (10.8.29.1, 10.8.58.6 and 10.8.58.8).



1. SIP MESSAGE 1: 10.8.29.1:5060 -> 10.8.58.4:5060

```

INVITE sip:conf100@10.8.58.4;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.29.1;branch=z9hG4bKacRHmJhMj
Max-Forwards: 70
From: <sip:100@10.8.8.10>;tag=1c352329022
To: <sip:conf100@10.8.58.4;user=phone>
Call-ID: 1792526528qlax@10.8.29.1
CSeq: 1 INVITE
Contact: <sip:100@10.8.29.1>
Supported: em,100rel,timer,replaces,path
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Type: application/sdp
Content-Length: 216
v=0
o=AudiocodesGW 663410 588654 IN IP4 10.8.29.1
    
```



```
s=Phone-Call
c=IN IP4 10.8.29.1
t=0 0
m=audio 6000 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
aptime:20
a=sendrecv
```

2. SIP MESSAGE 2: 10.8.58.4:5060() -> 10.8.29.1:5060()

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.8.29.1;branch=z9hG4bKacRHmJhMj
From: <sip:100@10.8.8.10>;tag=1c352329022
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c222574568
Call-ID: 1792526528qlax@10.8.29.1
CSeq: 1 INVITE
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Length: 0
```

3. SIP MESSAGE 3: 10.8.58.4:5060 -> 10.8.29.1:5060

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.29.1;branch=z9hG4bKacRHmJhMj
From: <sip:100@10.8.8.10>;tag=1c352329022
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c222574568
Call-ID: 1792526528qlax@10.8.29.1
CSeq: 1 INVITE
Contact: <sip:10.8.58.4>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Type: application/sdp
Content-Length: 216
v=0
o=AudiocodesGW 820775 130089 IN IP4 10.8.58.4
s=Phone-Call
c=IN IP4 10.8.58.4
t=0 0
m=audio 7160 RTP/AVP 8 96
a=rtpmap:8 pcma/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
aptime:20
a=sendrecv
```

4. SIP MESSAGE 4: 10.8.29.1:5060 -> 10.8.58.4:5060

```

ACK sip:10.8.58.4 SIP/2.0
Via: SIP/2.0/UDP 10.8.29.1;branch=z9hG4bKacbUrWtRo
Max-Forwards: 70
From: <sip:100@10.8.8.10>;tag=1c352329022
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c222574568
Call-ID: 1792526528qlax@10.8.29.1
CSeq: 1 ACK
Contact: <sip:100@10.8.29.1>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Length: 0
    
```

5. SIP MESSAGE 5: 10.8.58.6:5060 -> 10.8.58.4:5060

```

INVITE sip:conf100@10.8.58.4;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacfowEuut
Max-Forwards: 70
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 1 INVITE
Contact: <sip:600@10.8.58.6>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant 1000/v.4.60A.005.009
Content-Type: application/sdp
Content-Length: 313

v=0
o=AudiocodesGW 702680 202680 IN IP4 10.8.58.6
s=Phone-Call
c=IN IP4 10.8.58.6
t=0 0
m=audio 6000 RTP/AVP 4 8 0 110 96
a=rtpmap:4 g723/8000
a=fmtp:4 annexa=no
a=rtpmap:8 pcma/8000
a=rtpmap:0 pcmu/8000
a=rtpmap:110 AMR/8000/1
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
aptime:30
a=sendrecv
    
```

6. SIP MESSAGE 6: 10.8.58.4:5060 -> 10.8.58.6:5060

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacfowEuut
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c1673415884
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 1 INVITE
Supported: em,timer,replaces,path
    
```

```

Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Length: 0

```

7. SIP MESSAGE 7: 10.8.58.4:5060 -> 10.8.58.6:5060

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacfowEuut
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c1673415884
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 1 INVITE Contact: <sip:conf100@10.8.58.4>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Type: application/sdp
Content-Length: 236
v=0 o=AudiocodesGW 886442 597756 IN IP4 10.8.58.4
s=Phone-Call
c=IN IP4 10.8.58.4
t=0 0
m=audio 7150 RTP/AVP 4 96
a=rtpmap:4 g723/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
aptime:30
a=sendrecv

```

8. SIP MESSAGE 8: 10.8.58.6:5060 -> 10.8.58.4:5060

```

ACK sip:conf100@10.8.58.4 SIP/2.0
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacRRRZPXN
Max-Forwards: 70
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c1673415884
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 1 ACK
Contact: <sip:600@10.8.58.6>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant 1000/v.4.60A.005.009
Content-Length: 0

```

9. SIP MESSAGE 9: 10.8.58.8:5060 -> 10.8.58.4:5060

```

INVITE sip:conf100@10.8.58.4;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKaczJpxnnv
Max-Forwards: 70
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 1 INVITE

```

```

Contact: <sip:800@10.8.58.8>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant 1000/v.4.60A.005.009
Content-Type: application/sdp Content-Length: 236
v=0
o=AudiocodesGW 558246 666026 IN IP4 10.8.58.8
s=Phone-Call
c=IN IP4 10.8.58.8
t=0 0 m=audio 6000 RTP/AVP 4 96
a=rtpmap:4 g723/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:30
a=sendrecv
    
```

10. SIP MESSAGE 10: 10.8.58.4:5060 -> 10.8.58.8:5060

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKaczJpxnnv
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c3203015250
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 1 INVITE
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Length: 0
    
```

11. SIP MESSAGE 11: 10.8.58.4:5060 -> 10.8.58.8:5060

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKaczJpxnnv
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c3203015250
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 1 INVITE
Contact: <sip:conf100@10.8.58.4>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Type: application/sdp
Content-Length: 236
v=0
o=AudiocodesGW 385533 708665 IN IP4 10.8.58.4
s=Phone-Call
c=IN IP4 10.8.58.4
t=0 0
m=audio 7140 RTP/AVP 4 96
a=rtpmap:4 g723/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:30
a=sendrecv
    
```

12. SIP MESSAGE 12: 10.8.58.8:5060 -> 10.8.58.4:5060

```

ACK sip:conf100@10.8.58.4 SIP/2.0
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKacisqqyow
Max-Forwards: 70
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c3203015250
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 1 ACK
Contact: <sip:800@10.8.58.8>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Length: 0

```

13. SIP MESSAGE 13: 10.8.58.8:5060 -> 10.8.58.4:5060

```

BYE sip:conf100@10.8.58.4 SIP/2.0
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKackSIyGww
Max-Forwards: 70
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c3203015250
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 2 BYE
Contact: <sip:800@10.8.58.8>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Length: 0

```

14. SIP MESSAGE 14: 10.8.58.4:5060 -> 10.8.58.8:5060

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.58.8;branch=z9hG4bKackSIyGww
From: <sip:800@10.8.58.8>;tag=1c2419012378
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c3203015250
Call-ID: 150852731NDDC@10.8.58.8
CSeq: 2 BYE
Contact: <sip:conf100@10.8.58.4>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Length: 0

```

15. SIP MESSAGE 15: 10.8.58.6:5060 -> 10.8.58.4:5060

```

BYE sip:conf100@10.8.58.4 SIP/2.0
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacQypxnv1
Max-Forwards: 70
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c1673415884
Call-ID: 1008914574iYgW@10.8.58.6

```

```
CSeq: 2 BYE
Contact: <sip:600@10.8.58.6>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Length: 0
```

16. SIP MESSAGE 16: 10.8.58.4:5060 -> 10.8.58.6:5060

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.8.58.6;branch=z9hG4bKacQypxnv1
From: <sip:600@10.8.8.10>;tag=1c201038291
To: <sip:conf100@10.8.58.4;user=phone>;tag=1c1673415884
Call-ID: 1008914574iYgW@10.8.58.6
CSeq: 2 BYE
Contact: <sip:conf100@10.8.58.4>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40A.010.006
Content-Length: 0
```

20.1.2 Announcement Server

The device supports playing and recording of announcements (local Voice Prompts or HTTP streaming) and playing of Call Progress Tones over the IP network. Three different methods are available for playing and recording announcements:

- NetAnn for playing a single announcement (see 'NetAnn Interface' on page 414)
- MSCML for playing single or multiple announcements and collecting digits (see 'MSCML Interface' on page 415)

20.1.2.1 NetAnn Interface

The device supports playing announcements using NetAnn format (according to RFC 4240).

20.1.2.1.1 Playing a Local Voice Prompt

To play a single local Voice Prompt, the Application Server (or any SIP user agent) sends a regular SIP INVITE message with SIP URI that includes the NetAnn Announcement Identifier name. For example:

```
INVITE sip:annc@audiocodes.com; play=file://12 SIP/2.0
```

The left part of the SIP URI includes the string 'annc'. In the example above, the device starts playing announcement number 12 from the internal Voice Prompts file (file:// and http://localhost formats are supported). The NetAnn Announcement Identifier string is configured using the *ini* file (parameter NetAnnAnncID) or Web interface (see 'Configuring the IPmedia Parameters' on page 399). Sending a BYE request terminates the SIP session and stops the playing of the announcement. If the played Voice Prompt reaches its end, the device initiates a BYE message to notify the Application Server that the session has ended.

20.1.2.1.2 Playing using HTTP/NFS Streaming

To play a single announcement via HTTP or NFS streaming, the Application Server (or any SIP user agent) sends a regular SIP INVITE message with SIP URI that includes the NetAnn Announcement Identifier name. For example:

```
INVITE sip:annc@ac.com;
play=http://server.net/gem/Hello.wav SIP/2.0
```

The left part of the SIP URI includes the string 'annc' terminated by the IP address of the HTTP server, and the name and path of the file to be played. In the example above, the device starts playing the 'Hello.wav' file that resides in the folder 'server.net/gem'. The NetAnn Announcement Identifier string is configured using the *ini* file (parameter NetAnnAnnclD) or Web interface (see 'Configuring the IPmedia Parameters' on page 399). Sending a BYE request terminates the SIP session and stops the playing of the announcement. If the played announcement reaches its end, the device initiates a BYE message to notify the Application Server that the session is ended.



Notes:

- A 200 OK message is sent only after the HTTP connection is successfully established and the requested file is found. If the file isn't found, a 404 Not Found response is sent.
- To use NFS, the requested file system should be first mounted by using the NFS Servers table, see 'Configuring the NFS Settings' on page 127.

20.1.2.1.3 Supported Attributes

When playing announcements, the following attributes are available:

- **Repeat:** defines the number of times the announcement is repeated. The default value is 1. The valid range is 1 to 1000, or -1 (i.e., repeats the message forever).
- **Delay:** defines the delay (in msec) between announcement repetitions. The default value is 0. The valid range is 1 to 3,600,000.
- **Duration:** defines the total duration (in msec) the announcement(s) are played. The default value is 0 (i.e., no limitation). The valid range is 1 to 3,600,000.

For example:

```
INVITE sip:annc@ac.com;
play=http://server.net/gem/Hello.wav; repeat=5;delay=10000 SIP/2.0
```

20.1.2.2 MSCML Interface

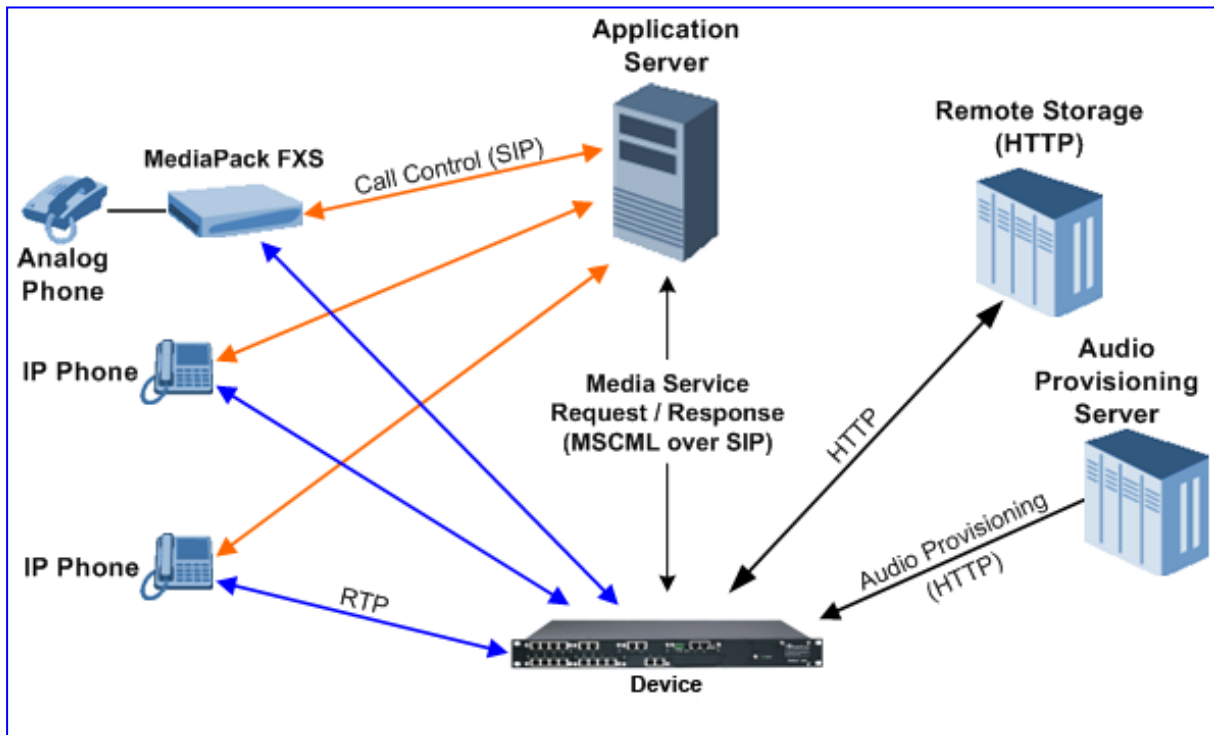
Media Server Control Markup Language (MSCML), according to IETF RFC 5022 is a protocol used in conjunction with SIP to provide advanced announcements handling. MSCML is implemented by adding an XML body to existing SIP INFO messages. Only a single message body (containing a single request or response) is allowed per message.

The device supports all the Interactive Voice Response (IVR) requirements for playing announcements, collecting digits, and recording (Play, PlayCollect, and PlayRecord).



Note: MSCML is only supported on devices operating with 128-MByte RAM size.

The following figure illustrates standard MSCML application architecture:



The architecture comprises the following components:

- **device:** Operating independently, the device controls and allocates its processing resources to match each application's requirements. Its primary role is to handle requests from the Application server for playing announcements and collecting digits.
- **Application Server:** An application platform that controls the call signaling. It interfaces with the device using MSCML. It instructs the media server to play announcements, collect digits and record voice streams.
- **Audio Provisioning Server (APS):** The APS is used for offline generation of .dat files of audio packages including audio files, audio sequences, and different languages for variable announcement playing. These can be later loaded to the device.
- **Remote Storage:** An HTTP server that contains less-frequently used voice prompts for playback and to which voice stream recording is performed.
- **IP Phones / MediaPack:** Client applications.

20.1.2.2.1 Operation

The APS server can be used to generate two files - the audio package as a VP.dat file, and an XML file (segments.xml) that contains indices to the announcements stored on the VP.dat file for playing announcements. These two files can be loaded to the device using the Web interface.

An alternative method uses the AutoUpdate mechanism as described in the *Product Reference Manual*. Both the vp.dat and segments.xml files that were previously created using the APS should be located on an external storage server (HTTP, FTP). At startup, the device fetches the files from the remote storage. By using the AutoUpdate mechanism, the device periodically checks if new files are posted to the remote server and fetches these files.

The Application server communicates with the device using MSCML Requests (sent by the Application server), as shown in the example below:

```
<?xml version="1.0" encoding="utf-8"?>
  <MediaServerControl version="1.0">
    <request>
      ... request body ...
    </request>
  </MediaServerControl>
```

The device uses MSCML Responses (i.e., sent by the device) to reply to the Application server, as shown in the example below:

```
<?xml version="1.0" encoding="utf-8"?>
  <MediaServerControl version="1.0">
    <response>
      ... response body ...
    </response>
  </MediaServerControl>
```

To start an MSCML IVR call, the Application server (or any SIP user agent) sends a regular SIP INVITE message with a SIP URI that includes the MSCML Identifier name. For example:

```
INVITE sip:ivr@audiocodes.com SIP/2.0
```

The left part of the SIP URI includes the MSCML Identifier string 'ivr', which can be configured using the *ini* file (parameter MSCMLID) or Web interface (see 'Configuring the IPmedia Parameters' on page 399).

After a call is established, SIP INFO messages are used to carry MSCML requests and responses. An INFO message that carries an MSCML body is identified by its content-type header that is set to 'application/mediaservercontrol+xml'.

Note that IVR requests are not queued. Therefore, if a request is received while another is in progress, the device stops the first operation and executes the new request. The device generates a response message for the first request and returns any data collected up to that point. If an application is required to stop a request in progress, it issues a <Stop> request. This request also causes the device to generate a response message.

The device supports basic IVR functions of playing announcements, collecting DTMF digits, and voice stream recording. These services are implemented using the following Request and Response messages:

- <Play> for playing announcements
- <PlayCollect> for playing announcements and collecting digits
- <PlayRecord> for playing announcements and recording voice
- <Stop> for stopping the playing of an announcement

The device sends a Response to each Request that is issued by the Application server.

The <Play>, <PlayCollect>, and <PlayRecord> messages are composed of two sections: Attributes and a Prompt block (the request can contain several different Prompt blocks). The Attributes section includes several request-specific parameters. The Prompt block section itself is also composed of two sections: prompt-specific parameters and audio segments (audio / variable). The (optional) prompt-specific parameters include:

- *locale*: defines the language in which the prompt block is played (supported for local files only). For more information on language usage, refer to the *Audio Provisioning*

Server User's Manual (LTRT-971xx).

- *baseurl*: defines a URL address that functions as a prefix to all audio segment URLs in the Prompt block.

The Prompt block contains references to one or more audio segments. The following audio segment types are available:

- **Physical Audio Segments:** These are physical audio files that are located either locally (on-blade) or on an external HTTP server. If the file is located on-blade, the reference to it is by using one of the following syntaxes:

'file://x', 'file:///x', 'file:///x' or 'http://localhost/x'

Where x stands for the file identifier (the ID or alias given by the APS server for local files; or the file's URL in for HTTP streaming).

- **Variables:** These are audio segments whose value is determined at run time. They are defined in the request as a <type, subtype, value> tuple. The device transforms the variable data to voice. To support variable playing, APS server support is mandatory. Available variable types are (subtypes in parenthesis): date (DMY - day month year; MDY - month day year - default), duration, month, money (USD), number (crd, ord), digit (gen, ndn) silence, string, time (t12, t24) and weekday. It is also possible to store audio files that are required to play supported types of phrases (e.g., dates and times) on an off-board system. This is beneficial in scenarios where the device's on-board storage limit has been reached, and thus, additional languages and audio can be stored off-board.
- **Sequences:** These are audio segments that consist of physical audio files and variables. These sequences can be defined using the APS server.

20.1.2.2.2 Operating with Audio Bundles

Voice prompts can be played from the device's local memory where they are stored as Audio bundles. An audio bundle is composed of a .dat file and an .xml file containing the information to properly parse the .dat file. Audio bundles are created through the APS and are then stored on a server supporting NFS or HTTP.

20.1.2.2.2.1 Uploading a Bundle to the Device

The audio bundle can be uploaded through FTP, NFS or HTTP. For more information, see the relevant Automatic Update chapter in the *Product Reference Manual*.

To upload a voice bundle to the device, the following *ini* file parameters should be set:

```
APSEnabled = 1
AMSProfile = 1
VpFileUrl = 'url-dat-file/dat-file'
APSSegmentsFileUrl = 'url-xml-file/xml-file'
```

Where *url-dat-file* and *url-xml-file* relate to the location of the relevant .dat and .xml files, and *dat-file* and *xml-file* relate to the file names, as shown in the example below:

```
APSEnabled = 1
AMSProfile = 1
VpFileUrl = 'http://10.50.2.1/dat_files/vp.dat'
APSSegmentsFileUrl = 'http://10.4.2.5/segments/segments.xml'
```

You can upload a bundle to the device using one of the following methods:

- Loading an ini file as described above, and then resetting the device (hard reset). Optionally, you can configure parameters through Web interface or using SNMP, and then burn parameters to flash and reset the device through Web or SNMP (soft reset).
- Adding the following *ini* file parameter to periodically upload the .dat and .xml files:

```
AutoUpdateFrequency = 100           // updating is performed every
100 minutes.
```

For more information, refer to Automatic Updates in the *Product Reference Manual*.

- Using SNMP to trigger an immediate upload of the files by setting `acSysActionSetAutoUpdate` to true.



Note: When uploading files through HTTP, if the names of the file that are already loaded to the device and the file intended to be uploaded are the same, time stamps of the old file and the new file should differ.

You can be notified on the outcome of an operation in two ways:

- Syslog messages – Informative Syslog messages are supplied when the operation has succeeded or failed. On operation failure, resort to first analyzing these messages.
- SNMP traps - Similar messages are also supplied via SNMP traps. For more information refer to the *Product Reference Manual*.

20.1.2.2.3 Playing Announcements

A <Play> request is used to play an announcement to the caller. Each <Play> request contains a single Prompt block and the following request-specific parameters:

- *id*: an optional random number used to synchronize request and response.
- *prompturl*: a specific audio file URL that is used in addition to the references in the Prompt block. This audio file is the first to be played.

An example of an MSCML <Play> Request that includes local and streaming audio files as well as variables is shown below:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <request>
    <play id="123">
      <prompt>
        <audio url="http://localhost/1"/>
        <variable type="digits" value="284"/>
        <variable type="silence" value="1"/>
        <audio url="http://10.3.0.2/aa.wav"/>
        <audiourl="nfs://10.3.0.3/prov_data/bb.wav"/>
      </prompt>
    </play>
  </request>
</MediaServerControl>
```

20.1.2.2.4 Playing Announcements and Collecting Digits

The <PlayCollect> request is used to play an announcement to the caller and to then collect entered DTMF digits. The play part of the <PlayCollect> request is identical to the <Play> request. The collect part includes an expected digit map. The collected digits are continuously compared to the digit map. Once a match is found, the collected digits are sent in a <PlayCollect> response. The digit map should be in MGCP format (the type value must be set to 'mgcpdigitmap').

For example:

```
<regex type="mgcpdigitmap" value="([0-1]xxx)">
</regex>
```

Each <PlayCollect> request contains the following request-specific parameters in addition to the Prompt block (all parameters are optional):

- *id*: an optional random number used to synchronize request and response.
- *prompturl*: a specific audio file URL that is used in addition to the references in the prompt block. This audio file is the first to be played.
- *barge*: if set to 'NO', DTMF digits received during announcement playback are ignored. If set to 'YES', DTMF digits received during announcement playback stop the playback and start the digit collection phase.
- *firstdigittimer*: defines the amount of time (in milliseconds) the user does not enter any digits, after which a response is sent indicating timeout.
- *interdigittimer*: defines the amount of time (in milliseconds) the user does not enter any digits after the first DTMF digit is received, after which a response is sent indicating timeout.
- *extradigittimer*: used to enable the following:
 - Detection of command keys (ReturnKey and EscapeKey).
 - Not report the shortest match. MGCP Digitmap searches for the shortest possible match. This means that if a digitmap of (123 | 1234) is defined, once the user enters 123, a match is found and a response is sent. If ExtraDigitTimer is defined, the match can also be 1234 because the device waits for the next digits. To use ExtraDigitTimer, it must be defined in the request and you must add a "T" to the Digitmap (for example, 'xxT'). The ExtraDigitTimer is only used when a match is found. Before a match is found, the timer used is the InterDigitTimer. Therefore, if the ExtraDigitTimer expires, a "match" response reason is reported -- never a "timeout".
- *maxdigits*: defines the maximum number of collected DTMF digits after which the device sends a response.
- *cleardigits*: defines whether or not the device clears the digit buffer between subsequent requests.
- *returnkey*: defines a specific digit (including '*' and '#') which (when detected during a collection) stops the collection and initiates a response (that includes all digits collected up to that point) to be sent.
- *escapekey*: defines a specific digit (including '*' and '#') which (when detected during a collection) stops the collection and initiates a response (with no collected digits) to be sent.

An example is shown below of an MSCML <PlayCollect> Request that includes a sequence with variables and an MGCP digit map:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <request>
    <playcollect id="6379" barge="NO" returnkey="#">
      <prompt>
        <audio url="http://localhost/1">
          <variable type="silence" value="1"/>
          <variable type="date" subtype="mdy"
value="20041210"/>
        </audio>
      </prompt>
      <regex type="mgcpdigitmap" value="([0-
1]xxx)">
      </regex>
    </playcollect>
  </request>
</MediaServerControl>
```

An example is shown below of an MSCML <PlayCollect> Response:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <response request="playcollect" id="6478" code="200"
text="OK" digits="4563">
  </response>
</MediaServerControl>
```

20.1.2.2.5 Playing Announcements and Recording Voice

The <PlayRecord> request is used to play an announcement to the caller and to then record the voice stream associated with that caller. The play part of the <PlayRecord> request is identical to the <Play> request. The record part includes a URL to which the voice stream is recorded. This URL refers to an HTTP server.

Each <PlayRecord> request contains the following request-specific parameters in addition to the Prompt block (all parameters except 'recurl' are optional):

- *id*: an optional random number used to synchronize request and response.
- *prompturl*: a specific audio file URL that is used in addition to the references in the prompt block. This audio file is the first to be played.
- *barge*: if set to 'NO', DTMF digits received during announcement playback are ignored. If set to 'YES', DTMF digits received during announcement playback stop the playback and start the recording phase.
- *cleardigits*: defines whether or not the device clears the digit buffer between subsequent requests.
- *escapekey*: defines a specific digit (including "*" and "#") which (when detected during any phase) stops the request and initiates a response.
- *recurl*: the URL on the external storage server to which the RTP stream is sent for recording. This is a mandatory parameter.
- *mode*: defines if the recording 'overwrites' the existing file or 'appends' to it.
- *initsilence*: defines how long to wait for initial speech input before terminating the recording. This parameter may take an integer value in milliseconds.

- *endsilence*: defines how long the device waits after speech has ended to stop the recording. This parameter may take an integer value in milliseconds.
- *duration*: the total time in milliseconds for the entire recording. Once this time expires, recording stops and a response is generated.
- *recstopmask*: defines a digit pattern to which the device compares digits detected during the recording phase. If a match is found, recording stops and a response is sent.

An example is shown below of an MSCML <PlayRecord> Request:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <request>
    <playrecord id="75899" barge="NO"
    Recurl=nfs://10.11.12.13/save/recordings/11.wav>
      <prompt>
        <audio url="nfs://100.101.102.103/45">
          <variable type="date" subtype="mdy"
          value="20041210"/>
        </audio>
      </prompt>
    </playrecord>
  </request>
</MediaServerControl>
```

An example is shown below of an MSCML <PlayRecord> Response:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <response request="playrecord" id="75899" code="200"
  text="OK" reclength="15005">
  </response>
</MediaServerControl>
```

20.1.2.2.6 Stopping the Playing of an Announcement

The Application server issues a <stop> request when it requires that the device stops a request in progress and not initiate another operation. The only (optional) request-specific parameter is id.

The device refers to a SIP re-INVITE message with hold media (c=0.0.0.0) as an implicit <Stop> request. The device immediately terminates the request in progress and sends a response.

An example is shown below of an MSCML <Stop> Request:

```
<?xml version="1.0" encoding="utf-8"?>
<MediaServerControl version="1.0">
  <request>
    <stop id="123">
    </stop>
  </request>
</MediaServerControl>
```

20.1.2.2.7 Relevant Parameters

The following parameters (described in 'IP Media Parameters' on page 751) are used to configure the MSCML:

- AmsProfile = 1 (mandatory)
- AASPackagesProfile = 3 (mandatory)
- VoiceStreamUploadMethod = 1 (mandatory)
- EnableVoiceStreaming = 1 (mandatory)
- MSCMLID (default="ivr")
- AmsPrimaryLanguage (default="eng")
- AmsSecondaryLanguage (default="heb")
- When using APS:
 - HeartBeatDestIP
 - HeartBeatDestPort
 - HeartBeatIntervalmsec
- When using AutoUpdate:
 - VPFileURL
 - APSSegmentsFileUrl
 - AutoUpdateFrequency / AutoUpdatePredefinedTime

20.1.2.2.8 Signal Events Notifications

The device supports Signal Events Notifications as defined in RFC 4722/5022 - MSCML. MSCML defines event notifications that are scoped to a specific SIP dialog or call leg. These events allow a client to be notified of various call progress signals. Subscriptions for call leg events are performed by sending an MSCML <configure_leg> request on the desired SIP dialog. Call leg events may be used with the MSCML conferencing or IVR services. Using the Signal Notifications, the device can report the following events:

Table 20-2: Reportable Events

Type	Subtype
AMD	<ul style="list-style-type: none"> ▪ voice ▪ automata ▪ silence ▪ unknown
CPT	<ul style="list-style-type: none"> ▪ SIT-NC ▪ SIT-IC ▪ SIT-VC ▪ SIT-RO ▪ busy ▪ reorder
FAX	<ul style="list-style-type: none"> ▪ CED ▪ CNG ▪ modem

Below is an example:

```
<?xml version="1.0"?>
<MediaServerControl version="1.0">
  <request>
    <configure_leg>
      <subscribe>
        <events>
          <signal type="amd" report="yes"/>
        </events>
      </subscribe>
    </configure_leg>
  </request>
</MediaServerControl>

<?xml version="1.0"?>
<MediaServerControl version="1.0">
  <notification>
    <signal type="amd" subtype="voice"/>
  </notification>
</MediaServerControl>
```

20.1.2.3 Voice Streaming

The voice streaming layer provides you with the ability to play and record different types of files while using an NFS or HTTP server.

20.1.2.3.1 Voice Streaming Features

The following subsections summarize the Voice Streaming features supported on HTTP and NFS servers, unless stated otherwise.

20.1.2.3.1.1 Basic Streaming Play

You may play a .wav, .au or .raw file from a remote server using G.711 coders.

20.1.2.3.1.2 Supported File Formats

The voice streaming layer provides support for .wav, .au, and .raw file formats. The maximum supported header size of the file is 150 bytes.

In .wav format, only mono mode and supported/known coders are supported. The maximum number of the non-data, non-fmt chunks can be up to 5.

20.1.2.3.1.3 Play from Offset

You may play a .wav, .au or .raw file from a given offset within the file. Offset can be both positive and negative relative to the file's length. A negative offset relates to an offset from the end of the file.

20.1.2.3.1.4 Remote File Systems

You may configure up to 16 remote file systems to operate with the system through NFS mounting.

20.1.2.3.1.5 Using Proprietary Scripts

You may use cgi or servlet scripts released with the version for recording to a remote HTTP server using the POST or PUT method.

20.1.2.3.1.6 Dynamic HTTP URLs

Voice streaming supports dynamic HTTP URLs. The following terminology is used:

- **Static audio content:** Traditional audio file URLs containing references to specific files (.wav, .au or .raw). For example: `http://10.50.0.2/qa/GOSSIP_ENG.wav`
- **Dynamic audio content:** URLs referencing to cgi scripts or servlets. For example: `http://10.50.0.2/cgi/getaudio.cgi?filename=DEFAULT_GREETING.raw&offset=0`

In the case of dynamic URLs, the device performs the GET command with the supplied URL and as a result, the servlet or cgi script on the Web server is invoked. The Web server responds by sending a GET response containing the audio.

The URL format can be as follows (RFC 1738 URLs, section 3.3):

```
http://<host>:<port>/<path>?<searchpart>
```

where,

- `:<port>` is optional.
- `<path>` is a path to a server-side script.
- `<searchpart>` is of the form: `key=value[&key=value]*`



Note: At least one key=value pair is required.

Another example of a dynamic URL is shown below:

```
http://MyServer:8080/prompts/servlet?action=play&language=eng&file=welcome.raw&format=1
```

(See also RFC 2396 URI: Generic Syntax.)

The servlet or cgi script can respond by sending a complete audio file or a portion of an audio file. The device skips any .wav or .au file header that it encounters at the beginning of the response. The device does not attempt to use any information in the header. For example, the device does not use the coder from the header. Note however, that the coder may be supplied through Web or *ini* file parameters.

20.1.2.3.1.7 Play LBR Audio File

You may play a file using low bit rate coders for .wav and .raw files.



Note: This feature is relevant for both NFS and HTTP.

20.1.2.3.1.8 Basic Record

You may record a .wav, .au or .raw files to a remote server using G.711 coders.



Note: This feature is relevant for both NFS and HTTP.

20.1.2.3.1.9 Remove DTMF Digits at End of Recording

You may configure a recording to remove the DTMF received at the end, indicating an end of a recording.



Note: This feature is relevant for both NFS and HTTP.

20.1.2.3.1.10 Record Files Using LBR

You may record a file using low bit rate coders for .wav and .raw files.



Notes: This feature is relevant for both NFS and HTTP.

20.1.2.3.1.11 Modifying Streaming Levels Timers

Several parameters enable the user to control streaming level timers for NFS and HTTP and also the number of data retransmission when using NFS as the application layer protocol:

- **General command timeout – ServerRespondTimeout:** Defines the maximal time a command or respond may be delayed. This relates both to HTTP commands (GET, PUT, POST, HEAD etc.) and to NFS commands (create, lookup, read, write etc.).
- **Recording packet overruns timer – StreamingRecordingOverRunTimeout:** An overrun condition is one in which the device sends data to the server but does not receive responds from the server acknowledging that it received the data. Overruns relate to recording data to a remote server and result with "holes" in the recording. The streaming level aborts sessions containing consecutive overruns as derived from this timer. You may set the timer to longer periods than the default value, thereby enabling the device to be more "tolerant" to overrun conditions.
- **Playing packet underruns – StreamingPlayingUnderRunTimeout:** An underrun condition is one in which the device does not supply the DSPs with sufficient data, thus "starving" the DSPs. Underruns relate to playing data from a server to the device where, due to environmental conditions (usually network problems), the data is not passed quickly enough. This condition results with broken data passed to the user. The streaming level aborts sessions containing consecutive underruns as derived from this timer. You may set the timer to longer periods than the default value, thereby enabling the device to be more "tolerant" to underrun conditions.
- **NFS command retransmission – NFSClientMaxRetransmission:** Defines the number of times an NFS command is retransmitted when the server side does not

respond. By default, the value is set to 0 and not used - instead, the number of retransmissions is derived from the server response timeout parameter and the current Recovery Time Objective (RTO) of the system.

These parameters may be configured using the *ini* file, Web interface, or SNMP.

20.1.2.3.2 Using File Coders with Different Channel Coders

The tables in the following subsections describe the support for different combinations of file coders (used for recording or playing a file) and channel coders (used when opening a voice channel).

The following abbreviations are used in the subsequent tables:

- **LBR:** Low Bit Rate Coder
- **PCMU:** G.711 μ -law coder
- **PCMA:** G.711 A-law coder
- **WB:** Linear PCM 16KHZ Wide Band Coder



Note: When recording with an LBR type coder, it is assumed that the same coder is used both as the file coder and the channel coder. Combinations of different LBR coders are currently not supported.

20.1.2.3.2.1 Playing a File

The table below lists the device's support of channel coders and file coders for playing a file.

Table 20-3: Coder Combinations - Playing a File

File Coder	File Type											
	.wav				.au				.raw			
	Channel Coder				Channel Coder				Channel Coder			
	PCMA	PCMU	LBR	WB	PCMA	PCMU	LBR	WB	PCMA	PCMU	LBR	WB
PCMA	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
PCMU	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
LBR	No	No	Yes	No	No	No	No	No	No	No	Yes	Yes

20.1.2.3.2.2 Recording a File

The table below lists the device's support of channel coders and file coders for recording a file.

Table 20-4: Coder Combinations - Recording a File

File Coder	File Type											
	WAV				AU				RAW			
	Channel Coder				Channel Coder				Channel Coder			
	PCMA	PCMU	LBR	WB	PCMA	PCMU	LBR	WB	PCMA	PCMU	LBR	WB
PCMA	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No
PCMU	Yes	Yes	Yes	No	Yes	Yes	Yes	No	Yes	Yes	Yes	No
LBR	No	No	Yes	No	No	No	No	No	No	No	No	No

20.1.2.3.3 Maximum Concurrent Playing and Recording

For details on maximum concurrent playing and recording, refer to the *Release Notes*.

20.1.2.3.4 LBR Coders Support

The following table describes the different low bit rate (LBR) coders and their support for .wav, .au, and .raw files.



Note: Coder support depends on the specific DSP template version installed on the device.

Table 20-5: LBR Coders and File Extension Support

Coder	.wav file	.raw file	.au file
G.726 (Rate 16)	Yes	Yes	No
G.726 (Rate 24)	Yes	Yes	No
G.726 (Rate 32)	Yes	Yes	No
G.726 (Rate 40)	Yes	Yes	No
G.723.1 (Rate 5.3)	Yes	Yes	No
G.723.1 (Rate 6.3)	Yes	Yes	No
G.729	Yes	Yes	No
GSM FR	Yes	Yes	No
MS GSM	Yes	Yes	No
GSM EFR	Yes	Yes	No
AMR (Rate 4.75)	No	Yes	No

Coder	.wav file	.raw file	.au file
AMR (Rate 5.15)	No	Yes	No
AMR (Rate 5.9)	No	Yes	No
AMR (Rate 6.7)	No	Yes	No
AMR (Rate 7.4)	No	Yes	No
AMR (Rate 7.95)	No	Yes	No
AMR (Rate 10.2)	No	Yes	No
AMR (Rate 12.2)	No	Yes	No
QCELP (Rate 8)	No	Yes	No
QCELP (Rate 13)	No	Yes	No

20.1.2.3.5 HTTP Recording Configuration

The HTTP record method (PUT or POST) is configured using the following offline *ini* parameter:

```
// 0=post (default), 1=put
VoiceStreamUploadMethod = 1
```

The default value is shown below:

```
VoiceStreamUploadPostUri =
"/audioupload/servlet/AcAudioUploadServlet"
```



Note: The PUT method disregards this string.

20.1.2.3.6 NFS Configuration Using the ini File

An example of an NFS configuration is shown below. In this example, NFS server 192.168.20.26 shares two file systems - one rooted at /PROV_data, and the other rooted at /opt/uas. NFSv3 is used for both remote file systems. The defaults for UID(0) and GID(1) are used.

```
[NFSServers]
FORMAT NFSServers_Index = NFSServers_HostOrIP,
NFSServers_RootPath, NFSServers_NfsVersion;
NFSServers 0 = 192.168.20.26, /PROV_data, 3;
NFSServers 1 = 192.168.20.26, /opt/uas, 3;
[\NFSServers]
```


Notes:

- The combination of Host/IP and Root Path should be unique for each row in the table. For example, there should be only one row in the table with a Host/IP of 192.168.1.1 and Root Path of /audio.
- To avoid terminating calls in progress, a row must not be deleted or modified while the system is accessing files on the remote NFS file system.
- An NFS file server can share multiple file systems. There must be a separate row in this table for each remote file system shared by the NFS file server that needs to be accessed by this system.
- For further details, see 'Configuring the NFS Settings' on page [127](#).

20.1.2.3.7 Supported HTTP Servers

The following is a list of HTTP servers that are known to be compatible with AudioCodes voice streaming under Linux™:

- **Apache:** cgi scripts are used for recording and supporting dynamic URLs.
- **Jetty:** servlets scripts are used for recording and supporting dynamic URLs.
- **Apache tomcat:** using servlets.

20.1.2.3.7.1 Tuning the Apache Server

It is recommended to perform the following modifications in the http.conf file located in the apache conf/ directory:

- Define PUT script location: Assuming the put.cgi file is included in this package, add the following line for defining the PUT script (script must be placed in the cgi-bin/ directory):

```
Script PUT /cgi-bin/put.cgi
```

- Create the directory /the-apache-dir/perl (for example, /var/www/perl) and copy the CGI script to this directory. In the script, change the first line from c:/perl/bin/perl to your perl executable file (this step is required only if mod_perl is not included in your Apache installation).
- Keep-alive parameters: the following parameters must be set for correct operation with multiple POST requests:

```
KeepAlive On
MaxKeepAliveRequests 0 (unlimited amount)
```

- Using mode perl, fix the mod_perl to the following:

```
<IfModule mod_perl.c>
<Location /cgi-bin>
  SetHandler perl-script
  PerlResponseHandler ModPerl::Registry
  Options +ExecCGI
  PerlOptions +ParseHeaders
  Order allow,deny
  Allow from all
</Location>
</IfModule>
```

- Apache MPM worker: it is recommended to use the Multi-Processing Module implementing a hybrid multi-threaded multi-process Web server. The following configuration is recommended:

```
<IfModule worker.c>
ThreadLimit      64
StartServers     2
ServerLimit     20000
MaxClients      16384
MinSpareThreads 100
MaxSpareThreads 250
ThreadsPerChild 64
MaxRequestsPerChild 16384
</IfModule>
```

20.1.2.3.8 Supporting NFS Servers

The table below lists the NFS servers that are known to be compatible with AudioCodes Voice Streaming functionality.

Table 20-6: Compatible NFS Servers

Operating System	Server	Versions
Solaris™ 5.8 and 5.9	nfsd	2, 3
Fedora™ Linux™ 2.6.5-1.358	nfsd	2, 3
Mandrake™ Linux™ v2.4.22	nfsd	2, 3
Windows™ 2000	Services For Unix™ (SFU)	2, 3
Windows™ 2000	winnfsd	2 (See Note)
SCO UnixWare™ 7.1.1	nfsd	2, 3
Windows™ 2000	Cygwin nfsd	2 (See Note)



Note: Cygwin and winnfsd support only NFSv2.

20.1.2.3.8.1 Solaris-Based NFS Servers

If you are using a Solaris™-based NFS server, then the following `nfsd` configuration modification is recommended, especially if you are planning to support voice recording:

- Edit the file `/etc/default/nfs` and set the value of `NFSD_SERVERS` to $N*2$, where N is the maximum number of record and play sessions that you expect to have in progress at any one time.

The `NFSD_SERVERS` parameter controls the number of worker threads that the NFS daemon uses to satisfy requests. When a request arrives, a check is made for an idle worker thread. If an idle worker thread is available, then the request is passed to it. If an idle worker thread is unavailable, then a new one is created and the request is passed to it. If the limit in worker threads is reached, the request is queued until one of the existing worker threads is available. Queuing of NFS requests from a real-time application such as the media server should be avoided. Therefore, the `NFSD_SERVERS` parameter should be used to ensure there is an adequate number of worker threads.

The default value for `NFSD_SERVERS` is 1. Typically, the `/etc/default/nfs` file contains `NFSD_SERVERS` set to 16.

To determine how many worker threads are running on the NFS server, invoke the following command:

```
pstack `pgrep nfsd` | grep nfssys | wc -l
```

An idle NFS daemon process displays 1 `nfsd` thread.

- Directories are shared by placing an entry in the `/etc/dfs/dfstab` file. See the `share(1M)` and `share_nfs(1M)` main pages for information on the format of entries in the `dfstab` file. Note that read-write (`rw`) is the default behavior. If you are planning to record to the file system, ensure that the directory is shared as `rw`. Also ensure that the recording directory has `777` (`rwrxrwx`) permissions.

Below is an example `/etc/dfs/dfstab` file. Note that `/audio1` is shared as read-only, and `/audio2` is shared as read-write.

```
> cat /etc/dfs/dfstab
share -F nfs -o ro /audio1
share -F nfs /audio2
```

- Ensure that the `/etc/nfssec.conf` file is configured so that "sys" is the default security mode. You should see the following:

```
> cat /etc/nfssec.conf
none      0      -      -      -      # AUTH_NONE
sys       1      -      -      -      # AUTH_SYS
dh        3      -      -      -      # AUTH_DH
default   1      -      -      -      # default is AUTH_SYS
```

- If the systems administrator wishes to use a default other than `AUTH_SYS` in the `nfssec.conf` file, then you should add "sec=sys" to each line in the `dfstab` file that is to be shared with an AudioCodes system. For example:

```
> cat /etc/dfs/dfstab
share -F nfs -o sec=sys,ro /audio1
share -F nfs -o sec=sys /audio2
```


- To restart the nfs daemon on Solaris, invoke the following two commands:

```
> /etc/init.d/nfs.server stop
> /etc/init.d/nfs.server start
```

- To view a log of directories which were shared on the previous restart of the nfs daemon, type the sharetab file. For example:

```
> cat /etc/dfs/sharetab
/audio1 - nfs ro
/audio2 - nfs rw
```

Other useful Solaris™ commands include the following:

- dfmounts: displays shared directories, including a list of clients that have these resources mounted.
- dfshares: displays a list of shared directories.

20.1.2.3.8.2 Linux-Based NFS Servers

The AudioCodes device uses local UDP ports that are outside of the range of 0..IPPORT_RESERVED(1024). Therefore, when configuring a remote file system to be accessed by an AudioCodes device, use the insecure option in the /etc/exports file. The insecure option allows the nfs daemon to accept mount requests from ports outside of this range.

Without the insecure option, the following nfs daemon log is received:

```
rpc.mountd: refused mount request from <ip> for <dir> illegal port
28000
```

Without the insecure option, the following Syslog is received:

```
NFS mount failed, reason=permission denied IP=<ip> path=<dir>
state=waitForMountReply numRetries=0
```

For more information, see the exports(5) main page on your Linux server.

An example /etc/exports entry is shown below:

```
/nfsshare *(rw,insecure,no_root_squash,no_all_squash,sync)
```

20.1.2.3.9 Common Troubleshooting

Always inspect the Syslog for any problem you may encounter; in many cases, the cause appears there.

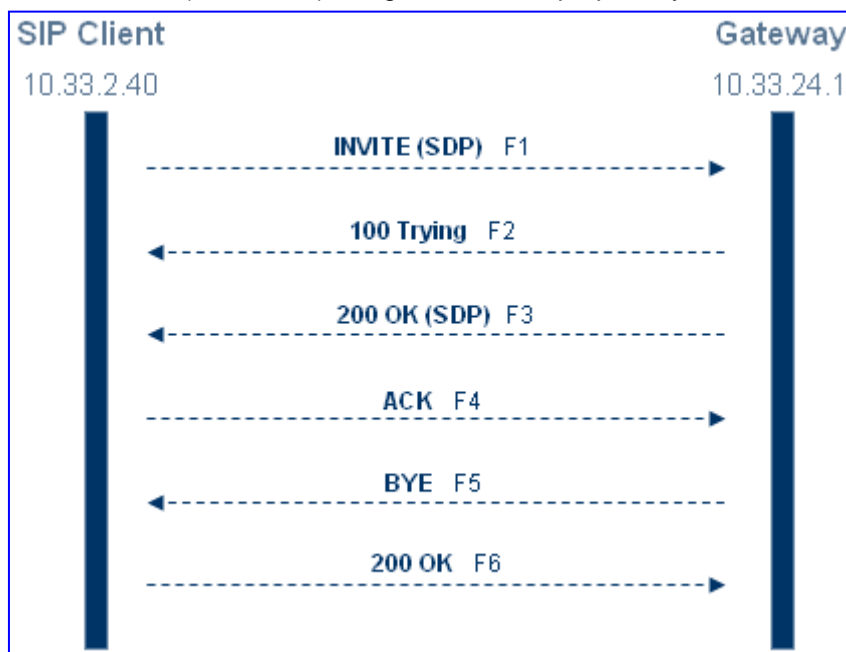
Table 20-7: Troubleshooting

Problem	Probable Cause	Corrective Action
General Voice Streaming Problems		
Attempts to perform voice streaming operations results in each Syslog containing the string: 'VS_STACK_NOT_ACTIVE'.	Voice streaming is not enabled.	Enable voice streaming by loading an <i>ini</i> file containing this entry: EnableVoiceStreaming = 1
HTTP Voice Streaming Problems		
The last half-second of an announcement is not played, or a record operation terminates abnormally and the Syslog displays the following: 'VSReceiveFromNetwork: VS_CONNECTION_WITH_SERVER_LOST'. (The problem has been experienced with Apache version 2.0.50 on Solaris 9.)	The Web server is closing the virtual circuit at unexpected times.	Increase the Apache KeepAliveTimeout config parameter. Try to increase it to 30 seconds or longer than the longest announcement or expected record session.
NFS Voice Streaming Problems		
Announcement is terminated prematurely and the Syslog displays the following: 'NFS request aborted ... networkError'.	The AudioCodes media server has lost communication with the NFS server. A network problem or some problem with the NFS server exists.	Fix the network problem or NFS server problem. Ensure that the NFS server is not over-loaded.
Unable to play announcements from an NFS server and each Syslog displays the following: 'Unable to create new request, file system not mounted' 'NFS mount error ...'	Either there is a problem with the NFS server, the network, or configuration of the media server or NFS server.	Fix the network problem or NFS server problem. Check the configuration on both the media server and the NFS server.
Record is terminated prematurely and the Syslog displays the following: 'VeData: no free buffers, req=16' 'Unable to play announNFS request aborted, reqid=16 cid=16 error=noRecordBufferError reqtype=vsHostRecord state=recTransfer'.	This occurs when the media server is receiving audio faster than it can save it to the remote NFS server. Either there is a problem with the NFS server, the network, or configuration of the media server or NFS server.	Fix the network problem or NFS server problem. Check the configuration on both the media server and the NFS server.

Problem	Probable Cause	Corrective Action
Remote file system is not being mounted and the Syslog displays the following: 'NFS mount failed, reason=permission denied IP=<ip> path=<dir> state=waitForMountReply numRetries=0';	The NFS server is not configured to accept requests on ports outside of the range 0...1024.	On a Linux NFS server, use the insecure option in the /etc/exports file (see Linux-Based NFS Servers on page 433).
All recording sessions are aborted at the same time with these Syslogs: 'NFS request aborted, reqid=209 cid=-1 error=writeReplyError reqtype=writeFile state=writeWait [File:NfsStateMachine.cpp ...]' 'NFS request aborted, reqid=186 cid=-1 error=writeReplyError reqtype=writeFile state=writeWait [File:NfsStateMachine.cpp ...]'	The file system on the NFS server is full.	Remove unwanted files on the file system.

20.1.2.4 Announcement Call Flow Example

The call flow, shown in the following figure, describes SIP messages exchanged between the device (10.33.24.1) and a SIP client (10.33.2.40) requesting to play local announcement #1 (10.8.25.17) using AudioCodes proprietary method.



1. SIP MESSAGE 1: 10.33.2.40:5060 -> 10.33.24.1:5060

```

INVITE sip:annc@10.33.24.1;play=http://10.3.0.2/hello.wav;repeat=2
SIP/2.0
Via: SIP/2.0/UDP 10.33.2.40;branch=z9hG4bKactXhKPQT
Max-Forwards: 70
From: <sip:103@10.33.2.40>;tag=1c2917829348
To: <sip:annc@10.33.24.1>
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 INVITE
Contact: <sip:103@10.33.2.40>
Supported: em,100rel,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-4.0 GA/v.4.0 GA
Content-Type: application/sdp
Content-Length: 215

v=0
o=AudiocodesGW 377662 728960 IN IP4 10.33.41.52
s=Phone-Call
c=IN IP4 10.33.41.52
t=0 0
m=audio 4030 RTP/AVP 4 0 8
a=rtpmap:4 g723/8000
a=rtpmap:0 pcmu/8000
a=rtpmap:8 pcma/8000
a=ptime:30
a=sendrecv
  
```

2. SIP MESSAGE 2: 10.33.24.1:5060 -> 10.33.2.40:5060

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 10.33.2.40;branch=z9hG4bKactXhKPQT
From: <sip:103@10.33.2.40>;tag=1c2917829348
To: <sip:annc@10.33.24.1>;tag=1c1528117157
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 INVITE
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40.010.006D
Content-Length: 0
  
```

3. SIP MESSAGE 3: 10.33.24.1:5060 -> 10.33.2.40:5060

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.33.2.40;branch=z9hG4bKactXhKPQT
From: <sip:103@10.33.2.40>;tag=1c2917829348
To: <sip:annc@10.33.24.1>;tag=1c1528117157
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 INVITE Contact: <sip:10.33.24.1>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,IN
FO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40.010.006D
Content-Type: application/sdp
Content-Length: 165

v=0
  
```

```

o=AudiocodesGW 355320 153319 IN IP4 10.33.24.1
s=Phone-Call
c=IN IP4 10.33.24.1
t=0 0
m=audio 7170 RTP/AVP 0
a=rtpmap:0 pcmu/8000
a=ptime:20
a=sendrecv

```

4. SIP MESSAGE 4: 10.33.240:5060 -> 10.33.24.1:5060

```

ACK sip:10.33.24.1 SIP/2.0
Via: SIP/2.0/UDP 10.33.2.40;branch=z9hG4bKacnNUEeKP
Max-Forwards: 70
From: <sip:103@10.33.2.40>;tag=1c2917829348
To: <sip:annc@10.33.24.1>;tag=1c1528117157
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 ACK
Contact: <sip:103@10.33.2.40>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-4.0 GA/v.4.0 GA
Content-Length: 0

```

5. SIP MESSAGE 5: 10.33.24.1:5060 -> 10.33.240:5060

```

BYE sip:103@10.33.2.40 SIP/2.0
Via: SIP/2.0/UDP 10.33.24.1;branch=z9hG4bKacFhtFbFR
Max-Forwards: 70
From: <sip:annc@10.33.24.1>;tag=1c1528117157
To: <sip:103@10.33.2.40>;tag=1c2917829348
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 BYE
Contact: <sip:10.33.24.1>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant 1000/v.5.40.010.006D
Content-Length: 0

```

6. SIP MESSAGE 6: 10.33.240:5060 -> 10.33.24.1:5060

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.33.24.1;branch=z9hG4bKacFhtFbFR
From: <sip:annc@10.33.24.1>;tag=1c1528117157
To: <sip:103@10.33.2.40>;tag=1c2917829348
Call-ID: 1414622340oZZq@10.33.2.40
CSeq: 1 BYE
Contact: <sip:103@10.33.2.40>
Supported: em,timer,replaces,path
Allow:REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Server: Audiocodes-Sip-Gateway-4.0 GA/v.4.0 GA
Content-Length: 0

```

20.1.3 Voice XML Interpreter

The device supports Voice Extensible Markup Language (VoiceXML) version 2.0. VXML is an XML-based scripting language used to prompt and collect information from callers. A VXML-based script may be used to control many types of interactive voice response (IVR) activities, including playing recorded announcements, collecting DTMF digits, recording a caller's voice, recognizing speech (i.e., automatic speech recognition or ASR), and synthesizing speech (i.e., text-to-speech or TTS). Its major goal is to bring the advantages of Web-based development and content delivery to interactive voice response applications.



Notes:

- VoiceXML is applicable only to Mediant 1000.
- Currently, ASR and TTS are not supported.

20.1.3.1 Features

VoiceXML offers the following features:

- VXML uses the AMS for enhanced audio features (i.e., playing prompts on a remote server, synthesized variables, enhanced digit patterns capabilities, different languages).
- Supports DTMF recognition.
- Supports recording of audio for later playback.
- Speech recognition: subscriber's speech is compared with voice grammars residing on an external speech server that is directed using the MRCP protocol) with matching words or phrases are returned as text strings.
- Text-to-Speech (TTS): regular text written in the IVR script is translated to speech and played to the user (the translation itself is done by an external server that is directed using the MRCP protocol).

20.1.3.2 Feature Key

VXML is protected by a Software Upgrade Key. However, if the device's Software Upgrade Key doesn't contain VXML, then VXML support is disabled. In such circumstances, upon trying to activate a VXML script, a Syslog message appears notifying the user that the VXML task was disabled. In addition, when the Software Upgrade Key doesn't contain VXML, the EnableVXML *ini* file parameter is ignored (i.e., although set to 1, VXML remains disabled).

20.1.3.3 VXML Scripts

Conceptually, there are two different types of VXML scripts that can be used (simultaneously or only one) by the device:

- **Dynamic scripts:** This script is downloaded as needed for an individual call and usually contains customized content for that particular call. When a call arrives, the device accesses a remote Web server to download a script. Once the script is downloaded, it's parsed, executed, and cleaned up at the end of the call.
- **Static scripts:** This script represents an application that can be used across many different callers. An example of such an application might be a drug prescription refill service where a prompt is played to the caller, the prescription number is obtained from the caller as speech or DTMF digits, and this data is then saved to an off-board database.

There are ramifications in using both these types of scripts. A dynamic script can be customized for each caller, but has to be downloaded and parsed for every call. However, static scripts are loaded once (although the system checks periodically for updates), parsed once, and then is re-used for each call. This results in better performance and using of fewer resources per call, because each call uses only what it needs of the parent script, and doesn't need its own copy of the full script.

Scripts are loaded initially through an INVITE message from the SIP Call Agent to the device. If the script is a static script, the device checks whether the file has already been loaded, and if so, it uses the existing script. Otherwise, the script is loaded to the device. Dynamic scripts are always loaded when requested.

A VXML script can trigger another VXML script to be loaded. An example of this is the VXML <goto> element, which can cause a transition to a different form in the same script, or to a completely different script. The script that is loaded as a result of the execution of the first script can be either dynamic or static. If the second script is a static script, the device checks whether it has already been loaded to the device and references that copy if it exists. Otherwise, the second script is loaded, parsed, and executed.

There are multiple ways in which VXML scripts may be loaded to the device. These include automatic update for static scripts (which allows for a script to be loaded using a remote FTP, HTTP, or NFS server), TFTP for static scripts (which allows a script to be loaded from a remote BootP/TFTP server), or HTTP for dynamic scripts. Refer to the appropriate sections for additional details.

The device can activate a VXML script using the VXMLID parameter in the Request-URI user part only, upon receipt of a regular INVITE message. For example:

```
Request-URI = <VXMLID>http://mydomain.com/myscript.cgi@host;
```

This is in addition to invoking VXML scripts on the receipt of SIP Request-URIs such as:

```
<VXMLID>@host;voicexml= http://...
```

This feature is supported for IP-to-Tel and Tel-to-IP calls. For specified dialed phone numbers, the user part can be manipulated by adding a VXML script path. For example, upon receipt of the INVITE request, INVITE sip:100@myhost, the device can be configured to manipulate (using the IP to Tel Manipulation table) the Request-URI user part to voicexml=http://myhost.com/script.cgi@myhost.

20.1.3.4 Proprietary Extensions

To provide the functionality intended by the VXML specification and to extend the functionality of the VXML specification, some proprietary extensions have been included in the AudioCodes VXML Interpreter. These extensions are discussed in the following sections and are intended to enable a VXML script to make use of the advanced audio capabilities provided by the device.

20.1.3.4.1 Record

As the device doesn't provide the ability to record 'on-board', it is necessary to record a caller's speech by streaming the audio to either an external NFS server. There are two additional attributes for the VXML <record> element that can be used to specify the off-board file name as well as the streaming mechanism for recording speech.

- "dest" attribute for <record>, which refers to a fully specified URL. An example of this is the following script:

```
<?xml version="1.0"?>
<vxml version="2.0" xmlns="http://www.w3.org/2001/vxml">
<form id="form1">
  <record name="msg" finalsilence="3000ms" maxtime="60s"
dtmfterm="true"
dest="http://192.168.1.2/recordings/greetings/callersspeech.wav">
  <audio src= "http://192.168.1.2/prompts/recordprompt.wav"/>
  <filled>
    <audio src = "http://192.168.1.2/prompts/confirm.wav"/>
    <audio src= "http://192.168.1.2/
greetings/callersspeech.wav"/>
    <exit/>
  </filled>
  <noinput>
    <audio src=
"http://192.168.1.2/prompts/recordprompt2.wav "/>
    <reprompt/>
  </noinput>
</record>
</form>
</vxml>
```

In this example, the "dest" attribute of the <record> element specifies that the caller's speech must be streamed with HTTP to the system with IP address 192.168.1.2, and stored in a file called "callersspeech.wav" on that system.

- The "destexpr" attribute provides an alternative to the "dest" attribute. The "destexpr" attribute is evaluated during runtime to determine where to store the caller's speech. The following is an example script illustrating its usage:

```
<?xml version="1.0"?>
<vxml version="2.0" xmlns="http://www.w3.org/2001/vxml">
<var name="recordpath" expr =
"'http://192.168.1.2/recordings/greetings/'"/>
<form id="form1">
  <record name="msg" finalsilence="3000ms" maxtime="60s"
dtmfterm="true" destexpr="recordpath + 'callersspeech.wav'">
  <audio src= "http://192.168.1.2/prompts/recordprompt.wav"/>
  <filled>
    <audio src = "http://192.168.1.2/prompts/confirm.wav"/>
    <audio expr= " recordpath + 'callersspeech.wav'"/>
    <exit/>
  </filled>
  <noinput>
    <audio src=
"http://192.168.1.2/prompts/recordprompt2.wav"/>
    <reprompt/>
  </noinput>
</record>
</form>
</vxml>
```


20.1.3.4.2 Audio Extensions

The device provides a rich set of functionality for building and playing announcements using recorded audio files. This functionality includes the ability to play certain types of phrases such as date, time, and number based upon a specific languages grammar rules. The files used to build the announcements can be stored on the device, or can be stored off-board on an external file system.

To take advantage of the advanced announcement capabilities provided by the device, the AudioCodes resident VXML Interpreter provides some extensions to the VXML <audio> element. These extensions are discussed in the following sections.

For more information on provisioning audio for the device, refer to the *Audio Provisioning Server (APS) User's Manual*.

20.1.3.4.2.1 Local Audio

While not a true extension, it's possible to play audio files that reside on-board a device. The following is an example of how such an audio file can be referenced using a VXML <audio> element.

```
<audio src = "http://localhost/123"/>
```

This reference directs the VXML software to play the audio segment marked with identifier '123'.

Using this method of access, the advanced audio structures defined by the AudioCodes Audio Provisioning Server (APS) can be referenced. While these various structures are outside the scope of the current document, they include sets, sequences, and multi-language variables. For more information on these advanced audio structures, refer to the *Audio Provisioning Server (APS) User's Manual*.

20.1.3.4.2.2 Say-as Tag for the Audio Element

While the VXML <say-as> tag is typically used as a directive to a text-to-speech engine in association with a VXML <prompt> element, the AudioCodes resident VXML Interpreter allows the <say-as> tag to also be used with the <audio> element. In this context, the <say-as> tag directs the VXML Interpreter to play phrases such as dates and times using provisioned audio files. The following is an example of an <audio> element using the <say-as> extension:

```
<audio> <say-as interpret-as="date"> 20080704 </say-as> </audio>
```

This example assumes that the device has been provisioned with the appropriate audio to play this example. The <audio> element in the example directs the VXML Interpreter to announce the date "July 4th, 2008".

The following table lists the supported phrase types, any valid subtypes for the phrases, the expected input format for each phrase type, and any notes for the various phrase types.

Table 20-8: Say-as Phrase Types

Say-as Token	Variable Type	Variable Subtype	Variable Input Format	Note
date	date	None supported	yyyymmdd	Dates are always announced according to

Say-as Token	Variable Type	Variable Subtype	Variable Input Format	Note
				the grammar rules of the language.
duration	duration	None supported	The input is up to 10 digits, with the value representing the duration in seconds.	Duration is always announced as hours, minutes, and seconds.
currency	money	Three-character ISO currency code. There is a specific set of currencies supported by the device, which are documented in Audio Provisioning Server (APS) User's Manual: Audio Files.	The input is up to 10 digits.	The number is converted appropriately to the currency in question. A value of 1234 in US Dollars, for example, is spoken as 12 dollars and 34 cents. The same input as Yen would be 1 thousand, 234 Yen.
number	number	cardinal	Up to 10 digits.	Integer
number:cardinal	number	cardinal	Up to 10 digits.	
number:ordinal	number	ordinal	Up to 10 digits.	Range of supported ordinal numbers varies by language, as to whether a certain ordinal number is supported by the language.
number:digits	digits	generic	A string of up to 64 digits including 0-9, * and #.	
telephone	digits	generic	A string of up to 64 digits including 0-9, * and #.	
telephone:ndn	digits	North American DN	Must be 10 digits 0-9.	
telephone:gen	digits	generic directory number	A string of up to 64 digits including 0-9, *, and #.	
time	time	t24	hhmm	24 hour time.
time:t12	time	t12	hhmm	
time:t24	time	t24	hhmm	

Below are two examples that direct the device to announce the cardinal number 1000.

```
<audio> <say-as interpret-as="number"> 1000 </say-as> </audio>
<audio> <say-as interpret-as="number:cardinal"> 1000 </say-as>
</audio>
```

In the example below, the device is directed to announce the string as a North American directory number. The output is “eight hundred, five five five, one two one two”. A few moments of silence are inserted at the points in the phrase indicated by commas.

```
<audio> <say-as interpret-as="telephone:ndn"> 8005551212 </say-as>
</audio>
```

In the example below, the device outputs the announcement “one million two hundred twenty thousand seven hundred dollars and fifteen cents”:

```
<audio> <say-as interpret-as="currency:usd"> 122070015 </say-as>
</audio>
```

20.1.3.4.2.3 Supplying Values to Provisioned Variables

As mentioned previously, the APS provides the capability to provision several types of advanced audio structures, including multi-language variables. A multi-language variable is an instance of one of the supported phrase types such as date and time. The APS assigns a numeric segment identifier to each variable, and the value for the variable can be provided at runtime. VXML doesn't define any capability for passing a value to a variable, therefore, the AudioCodes VXML Interpreter provides an extension to support this capability.

Below is an example that demonstrates this capability. Assume that a variable of type “date” has been provisioned on the APS, and the variable has been assigned segment identifier 17.

```
<audio src="http://localhost/17?var=20080120"/>
```

In this example, the device outputs the date “January 20th, 2008”.

20.1.3.4.2.4 Supplying Selector Values to Provisioned Variables and to Say-as Phrases

Another concept supported by the device is “selectors”. A selector is a keyword and value pair that is used by the device software to build announcements. There can be many combinations of keywords and values used for selectors, but the keyword “lang” and a language code are especially useful because this pair of tokens can be used to vary the language for announcements. For example, to announce the date from the previous example in French, below is syntax using the previous example along with a selector that builds the French announcement:

```
<audio src="http://localhost/17?var=20070620&sel=lang=fr"/>
```

More than one selector in an <audio> element can exist. In the example below, the language is French and gender selector with the value “female” is also specified:

```
<audio
src="http://localhost/17?var=20070620&sel=lang=fr&gender=F"/>
```

Selectors can also be useful in combination with <say-as> elements. For example, the following illustrates making the same announcement from the previous example using a <say-as> element:

```
<audio src="?sel=lang=fr&gender=F"> <say-as interpret-as="date">
20070620 </say-as> </audio>
```

For more information on available selectors, refer to the *Audio Provisioning Server (APS) User's Guide*.

20.1.3.4.3 Language Identifier Support

The AudioCodes resident VXML engine supports language identifiers as specified by RFC 3066. However, when accessing audio resident on the device using the proprietary extensions described earlier, the country code portion of the identifier is ignored. In addition, the language code portion of the identifier supports the languages listed in the table below.

Table 20-9: Support for Language Code Portion of Identifier

Language Code	Language
bd	Belgian Dutch
ca	Catalan
cs	Czech
de	German
el	Greek
en	English
es	Spanish
eu	Basque
fr	French
gl	Gallegan
he	Hebrew
hi	Hindi
it	Italian
ja	Japanese
ko	Korean
ms	Malay
nl	Netherlands Dutch
pt	Portuguese
ru	Russian
sw	Swedish
th	Thai
tl	Tagalog
tr	Turkish

Language Code	Language
vi	Vietnamese
yu	Cantonese
zh	Mandarin

20.1.3.5 Combining <audio> Elements

The VXML specification supports multiple <audio> elements nested within other elements such as prompts. An example demonstrating this functionality which includes the AudioCodes extensions is useful to show how multiple components can be combined to create a single announcement.

The following example shows how an announcement can be constructed that says “Welcome to Acme Corporation. Today’s date is June 20th, 2010. Today’s special is large widgets, two for ten dollars.” For the sake of the example, assume the following:

- “Welcome to Acme Corporation” and “Today’s special is large widgets, two for ten dollars” are stored on an external file system and is played using HTTP streaming.
- “Today’s date is” is a recording provisioned on the APS as segment 99.
- “June 20th, 2008” is a multi-language variable announcement made up of multiple recordings provisioned on the APS.

```
<prompt bargein="false">
  <audio src = "http://192.168.1.2/announcements/welcome.wav" />
  <audio src = "http://localhost/99"/>
  <audio src="?sel=lang=en"> <say-as interpret-as="date">
20080620 </say-as> </audio>
  <audio src =
"http://192.168.1.2/announcements/todaysspecial.wav" />
</prompt>
```

20.1.3.6 Notes Regarding Non-compliant Functionality

The AudioCodes resident VXML Interpreter doesn't asynchronously throw events as described in the VXML Specification. For example, if the clear element tries to clear an element within a script and that element does not exist, the VXML Specification specifies that the Interpreter should throw an “error.badfetch” event. In contrast, the AudioCodes Interpreter logs an appropriate error to the syslog for the device and the script exits. The VXML Interpreter behaves similarly for software errors in general such as running out of memory resources, trying to access non-existent audio files, etc. The impact of not throwing events asynchronously can be minimized by carefully testing all code paths for a VXML script before its deployment.

20.1.3.7 Supported Elements and Attributes

The following status legend should be referenced for all tables in the following subsections:

- **NS:** Not Supported
- **PS:** Partially Supported
- **S:** Supported

20.1.3.7.1 VoiceXML Supported Elements and Attributes

Table 20-10: VoiceXML Supported Elements and Attributes

Element	Parameter	Max Size	Shadow Variable	Status	Comments
<assign>				S	
	name	64		S	
	expr	128		S	
<audio>				S	The AudioCodes audio element has proprietary extensions in addition to attributes from the standard to support on-board audio variables.
	src	256		S	
	fetchtimeout			NS	
	fetchhint			NS	Default behavior is "safe"; fetch document when it's needed.
	maxage			NS	
	maxstale			NS	
	expr	128		S	
	catching			Ignored	1.0 VXML attribute not present in VXML 2.0.
<block>				S	
	name	32		S	
	expr	128		S	
	cond	64		S	
<catch>				S	
	event	64		S	
	count	numeric		S	
	cond	128		S	
<choice>				S	
	dtmf			S	
	accept			NS	
	next	256		S	
	expr	128		S	
	event	64		S	
	eventexpr	128		S	
	message			NS	

Element	Parameter	Max Size	Shadow Variable	Status	Comments
	messageexpr			NS	
	fetchaudio			NS	
	fetchtimeout			NS	
	fetchhint			NS	Default behavior is "safe"; fetch document when it's needed.
	maxage			NS	
	maxstale			NS	
<clear>				S	
	namelist	4 * 32		S	
<disconnect>				S	
<else>				S	
<elseif>				S	
	cond	128		S	
<enumerate>				NS	
<error>				S	
	count	numeric field		S	
	cond	128		S	
<exit>				S	
	expr	128		S	
	namelist	4 * 32		S	
<field>				S	
	name	32		S	
	expr	128		S	
	cond	128		S	
	type	enum		PS	Built-in grammars are supported for recognition against fields, but the match isn't spoken as the built-in type in text-to-speech.
	slot			NS	Default value is the variable name, thus, slot is not needed.
	modal	true/false		S	
		64	name\$.utterance	S	
		enum	name\$.inputmode	S	

Element	Parameter	Max Size	Shadow Variable	Status	Comments
		64	name\$.interpretation	S	
		numeric	name\$.confidence	S	
<filled>				S	
	mode			S	
	namelist	4 * 32		S	
<form>				S	
	id	32		S	
	scope	enum		S	
<goto>				S	
	next	256		S	
	expr	128		S	
	nextitem	32		S	
	expritem	128		S	
	fetchaudio			NS	
	fetchtimeout			NS	
	fetchhint			NS	
	maxage			NS	
	maxstale			NS	
<grammar>				S	
	version			S*	For voice grammars, this is passed to the speech recognition engine.
	xml:lang	5		S*	For voice grammars, this is passed to the speech recognition engine.
	mode			S	
	root			S	
	tag			S	
	xml:base			NS	
	src	256		S	
	scope	enum		S*	In this release, a document scope grammar isn't active in a dialog scope form.
	type	enum		PS	Built-in grammars are supported for recognition against fields, but the match is not spoken as the built-in

Element	Parameter	Max Size	Shadow Variable	Status	Comments
					type in text-to-speech.
	weight	numeric		S*	For voice grammars, this is passed to the speech recognition engine.
	fetchtimeout			NS	Voice grammars are maintained on the speech recognition server, not on device, thus this set of attributes that control caching of grammar doesn't apply.
	fetchhint			NS	Voice grammars are maintained on the speech recognition server, not on device, thus this set of attributes that control caching of grammar doesn't apply.
	maxage			NS	Voice grammars are maintained on the speech recognition server, not on device, thus this set of attributes that control caching of grammar doesn't apply.
	maxstale			NS	Voice grammars are maintained on the speech recognition server, not on device, thus this set of attributes that control caching of grammar doesn't apply.
<help>				S	
	count	numeric field		S	
	cond	128		S	
<if>				S	
	cond	128		S	
<initial>				NS	The initial element and all its attributes aren't supported in this release.
	name			NS	
	expr			NS	
	cond			NS	
<link>				S	
	next	256		S	
	expr	128		S	
	event	65		S	
	eventexpr	128		S	
	message			NS	
	messageexpr			NS	
	dtmf	31		S	
	fetchaudio			NS	

Element	Parameter	Max Size	Shadow Variable	Status	Comments
	fetchtimeout			NS	
	fetchhint			NS	Default behavior is "safe"; fetch document when it's needed.
	maxage			NS	
	maxstale			NS	
<log>				S	
	label	32		S	
	expr	128		S	
<menu>				S	
	id	32		S	
	scope	enum		S	
	dtmf	true/false		S	
	accept			NS	It's not obvious how to instruct the speech recognition engine that approximate matches are acceptable.
<noinput>				S	
	count	numeric		S	
	cond	128		S	
<nomatch>				S	
	count	numeric field		S	
	cond	128		S	
<object>				S	
	name	*		S	Since objects are developed for proprietary purposes as needed, attribute sizes aren't listed.
	expr			S	
	cond			S	
	classid			S	
	codebase			S	
	codetype			S	
	data			S	
	type			S	
	archive			S	
	fetchtimeout			NS	

Element	Parameter	Max Size	Shadow Variable	Status	Comments
	fetchhint			NS	Default behavior is "safe"; fetch document when it's needed.
	maxage			NS	
	maxstale			NS	
<option>				S	
	dtmf	31		S	
	accept			NS	It's not obvious how to instruct the speech recognition engine that approximate matches are acceptable.
	value	32		S	
<param>				S	
	name	32		S	
	expr	128		S	
	value	128		S	
	valuetype	enum		S	
	type	128		S	
<prompt>				S	
	bargein	true/false		S	
	bargeintype			PS	Speech barge-in is supported, but not hotword.
	cond	128		S	
	count	numeric		S	
	timeout	numeric		S	
	xml:lang	5			
	xml:base	256			
<property>				S	
	name	32		S	
	value	128		S	
<record>				S	
	name	32		S	
	expr	128		S	
	cond	128		S	
	modal			NS	Grammars are not supported, thus, modal doesn't apply.

Element	Parameter	Max Size	Shadow Variable	Status	Comments
	beep	true/false		S	Requires that a user-defined tone be added to the system. For an example, see 'Example of UDT 'beep' Tone Definition' on page 460. Refer to the Auxiliary Files section for additional details regarding creating user-defined tones.
	maxtime	time value		S	
	finalsilence	time value		S	
	dtmfterm			NS	DTMF and voice grammars aren't supported for record, but the termchar property can be used to terminate recordings.
	type			NS	The recorded audio format is specified by the file extension in the dest or destexpr attribute.
	dest	256		S*	Not part of the standard, either this attribute or destexpr are needed to specify the remote URL where the recorded audio is stored.
	destexpr	128		S*	Refer to previous item.
		numeric	name\$.duration	S	
			name\$.size	NS	As recorded audio is not stored onboard the device size is not available.
		1	name\$.termchar	S	
		true/false	name\$.maxtime	S	
<reprompt>				S	
<return>				S	
	event	64		S	
	eventexpr	128		S	
	message			NS	
	messageexpr			NS	
	namelist	4 * 32		S	
<script>				NS	The script element and all of its attributes are not supported.
	src			NS	
	charset			NS	
	fetchtimeout			NS	
	fetchhint			NS	
	maxage			NS	

Element	Parameter	Max Size	Shadow Variable	Status	Comments
	maxstale			NS	
<subdialog>				S*	Playing a prompt from a sub-dialog element is not supported in this release.
	name	32		S	
	expr	128		S	
	cond	128		S	
	namelist	4 * 32		S	
	src	256		S	
	srcexpr	128		S	
	method	enum		S	
	enctype			NS	
	fetchaudio			NS	
	fetchtimeout			NS	
	fetchhint			NS	Default behavior is "safe"; fetch document when it's needed.
	maxage			NS	
	maxstale			NS	
<submit>				S	
	next	256		S	
	expr	128		S	
	namelist	4 * 32		S	
	method	enum		S	
	enctype			NS	
	fetchaudio			NS	
	fetchtimeout			NS	
	Fetchhint			NS	Default behavior is "safe"; fetch document when it's needed.
	Maxage			NS	
	maxstale			NS	
	<throw>				S
Event		64		S	
eventexpr		128		S	

Element	Parameter	Max Size	Shadow Variable	Status	Comments	
	message			NS		
	messageexpr			NS		
<transfer>				S		
	Name			S		
	Expr			NS		
	Cond			S		
	Dest			NS	Only numbers.	
	destexpr			S		
	Bridge			S	Only blind transfer supported (false).	
	type			S	Only blind transfer supported (blind).	
	connecttimeout			NS		
	maxtime			NS		
	transferaudio			NS		
	Aai			NS		
	Aaiexpr			NS		
				name\$.duration	S	
				name\$.inputmode	S	
			name\$.utterance	S		
<value>				S		
	expr	128		S		
<var>				S		
	name	32		S		
	expr	128		S		
<transfer>	Name			S		
	Expr			NS		
	Cond			S		
	Dest			NS	Only numbers.	
	destexpr			S		
	Bridge			NS	Only Bridge = false	
	type			NS	Only type = blind	

Element	Parameter	Max Size	Shadow Variable	Status	Comments
	connecttimeout			NS	
	maxtime			NS	
	transferaudio			NS	
	Aai			NS	
	Aaiexpr			NS	
			name\$.duration	S	
			name\$.inputmode	S	
			name\$.utterance	S	
<value>				S	
	expr	128		S	
<var>				S	
	name	32		S	
	expr	128		S	
<vxml>				S	

20.1.3.7.2 SRGS and SSML Support

Note that elements associated with either the Speech Recognition Grammar Specification (SRGS) or Speech Synthesis Markup Language (SSML) are used to control the behavior of a remote speech engine for either speech recognition or text-to-speech. These elements would be passed from the VXML interpreter to the remote speech engine and are outside the scope of VXML.

20.1.3.7.3 VoiceXML Supported Properties

Table 20-11: VoiceXML Supported Properties

Platform Properties	Status	Equivalent <i>ini</i> file parameter or Notes
Recognizer		
confidencelevel	S	VxmlConfidenceLevel
Sensitivity	S	VxmlSensitivityLevel
speedvsaccuracy	S	VxmlSpeedVsAccuracy
Completetimeout	S	VxmlCompleteTimeout
incompletetimeout	S	VxmlInCompleteTimeout
maxspeechtimeout	S	VxmlMaxSpeechTimeout

Platform Properties	Status	Equivalent <i>ini</i> file parameter or Notes
DTMF Recognizer		
Interdigittimeout	S	VxmlInterDigitTimeout
Termtimeout	S	VxmlTermTimeout. Note that the system default is not 0 as directed in the specification for the protocol, but 3 seconds. This is to ensure digit collection functions correctly.
Termchar	S	VxmlTermChar
Prompt and Collect		
Bargein	S	VxmlBargeinAllowed
Bargeintype	NS	Regular speech vs hotword bargein
Timeout	S	VxmlNoInputTimeout
Fetching		
Audiofetchhint	NS	
Audiomaxage	NS	
Audiomaxstale	NS	
documentfetchhint	NS	
documentmaxage	NS	
documentmaxstale	NS	
grammarfetchhint	NS	
Grammarmaxage	NS	
Objectfetchhint	NS	
Objectmaxage	NS	
Objectmaxstale	NS	
Scriptfetchhint	NS	
Scriptmaxage	NS	
Scriptmaxstale	NS	
Fetchaudio	NS	
Fetchaudiodelay	NS	
fetchaudiominimum	NS	
Fetchtimeout	NS	
Miscellaneous		
Inputmodes	S	VxmlSystemInputModes. Note that the system default is 0 (DTMF) vs 2 (Voice and DTMF) as specified in the specification. This is because the majority of systems are expected to use DTMF collection and local or streamed announcements as opposed to text-to-speech and speech recognition.

Platform Properties	Status	Equivalent <i>ini</i> file parameter or Notes
Universals	NS	Universal grammars and behaviors such as help, cancel, and exit. Default is none.
Maxnbest	NS	Size of last result array

20.1.3.7.4 VoiceXML Variables and Events

Table 20-12: VoiceXML Variables and Events

Variable/Event Name	Status	Notes
Standard Session Variables		
session.connection.local.uri	S	
session.connection.remote.uri	S	
session.connection.protocol.name	S	
session.connection.protocol.version	S	The version is "2" (instead of "2.0").
session.connection.redirect	S	Redirect reason and screening information contains underscore "_" (instead of white space) between words.
session.connection.aai	S	
session.connection.originator	NS	
Standard Application Variables		
application.lastresult\$	S	The application.lastresult variables array is one element deep.
application.lastresult\$[i].confidence	S	
application.lastresult\$[i].utterance	S	
application.lastresult\$[i].inputmode	S	
application.lastresult\$[i].interpretation	S	
Pre-defined Events		
Note: while throwing and catching events from scripts are supported, throwing events asynchronously from within the interpreter (e.g., an event.badfetch) is currently not supported.		
catch	S	
connection.disconnect.hangup	NS	
connection.disconnect.transfer	NS	
exit	S	
help	S	
noinput	S	
nomatch	S	
maxspeechtimeout	S	
error.badfetch	PS	In most cases, the conditions that would cause this event are recognized during script parsing, thus, the script loading fails.

Variable/Event Name	Status	Notes
error.badfetch.http.response_code	NS	
error.badfetch.protocol.response_code	NS	
error.semantic	PS	
error.noauthorization	NS	
error.noresource	NS	
error.unsupported.builtin	NS	
error.unsupported.format	NS	
error.unsupported.language	NS	
error.unsupported.objectname	NS	Unsupported elements are recognized during initial parsing, thus, the script isn't executed, and no events are thrown.
error.unsupported.element	NS	Unsupported elements are recognized during initial parsing, thus, the script isn't executed, and no events are thrown.
Transfer Events		
connection.disconnect.hangup	NS	
connection.disconnect.transfer	NS	
Transfer Errors		
error.connection.noauthorization	NS	
error.connection.baddestination	NS	
error.connection.noroute	NS	
error.connection.noresource	NS	
error.connection.protocol.nnn	NS	
error.unsupported.transfer.blind	NS	
error.unsupported.transfer.bridge	NS	
error.unsupported.uri	NS	

20.1.3.7.5 ECMAScript Support

The following table describes the ECMAScript support that the AudioCodes resident VXML engine provides. As shown in the example below, all operands and operators in an expression must be separated by one or more ECMAScript whitespace characters.

```
<var name="orange" expr="var1 + 7"/>
```

Below is an example of incorrect formatting (i.e., not supported):

```
<var name="orange" expr="var1+7"/>
```

Table 20-13: ECMAScript Support

Operand/Operator	Examples	Status	Note
Whitespace chars	tab, vertical tab, form feed, and space	S	
Arithmetic Operators	+, ++, -, --, *, /, %	S	
Logical Operators	&&, , !	S	
Assignment Operators	=, +=, -=, *=, /=, %=, &=, ^=, =, <<=, >>=, >>>=	S	
Bitwise Operators	&, ^, , ~, <<, >>, >>>	S	
Comparison Operators	==, !=, >, >=. <, <=	S	
String Operators	+, +=	S	
Entity Reference Mapping The following is supported / required: Operator Entity Reference < < <= <= > >= >= >= && && Support for the '≤' and '≥' entities is currently not available.		S	
Null Literals	null	S	Section 7.8.1, ECMA-262 3rd Edition December, 1999
Boolean Literals	true, false	S	Section 7.8.2, ECMA-262 3rd Edition December, 1999
Numeric Literals		S	Section 7.8.3, ECMA-262 3rd Edition December, 1999
String Literals		S	Section 7.8.4, ECMA-262 3rd Edition December, 1999

20.1.3.8 Example of UDT 'beep' Tone Definition

The following is an example definition for 'beep' tone used for the <record> element:

```
#record beep tone
[CALL PROGRESS TONE #1]
Tone Type=202
Low Freq [Hz]=430
High Freq [Hz]=0
Low Freq Level [-dBm]=13
High Freq Level [-dBm]=0
First Signal On Time [10msec]=100
First Signal Off Time [10msec]=0
Second Signal On Time [10msec]=0
Second Signal Off Time [10msec]=0
Default Duration [msec]=350
```

20.1.3.9 Limitations and Restrictions

The maximal length of the VXML file is 65536 bytes.

21 Transcoding using Third-Party Call Control

The device supports transcoding using a third-party call control Application server. This support is provided by the following:

- Using RFC 4117 (see 'Using RFC 4117' on page 461)
- Using RFC 4240 - NetAnn Conferencing (see Using RFC 4240 - NetAnn 2-Party Conferencing on page 462)



Note: Transcoding can also be implemented using the IP-to-IP (IP2IP) application.

21.1 Using RFC 4117

The device supports RFC 4117 - Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc) - providing transcoding services (i.e., acting as a transcoding server). This is used in scenarios where two SIP User Agents (UA) would like to establish a session, but do not have a common coder or media type. When such incompatibilities are found, the UAs need to invoke transcoding services to successfully establish the session. Note that transcoding can also be performed using NetAnn, according to RFC 4240.

To enable the RFC 4117 feature, the parameter EnableRFC4117Transcoding must be set to 1 (and the device must be reset).

The 3pcc call flow is as follows: The device receives from one of the UAs, a single INVITE with an SDP containing two media lines. Each media represents the capabilities of each of the two UAs. The device needs to find a match for both of the media, and opens two channels with two different media ports to the different UAs. The device performs transcoding between the two voice calls.

In the example below, an Application Server sends a special INVITE that consists of two media lines to perform transcoding between G.711 and G.729:

```
m=audio 20000 RTP/AVP 0
c=IN IP4 A.example.com
m=audio 40000 RTP/AVP 18
c=IN IP4 B.example.com
```

21.2 Using RFC 4240 - NetAnn 2-Party Conferencing

Transcoding bridges (or translates) between two remote *network* locations, each of which uses a different coder and/or a different DTMF and fax transport types. The device supports IP-to-IP transcoding. It creates a transcoding call that is similar to a dial-in, two-party conference call. The SIP URI in the INVITE message is used as a transcoding service identifier. The transcoding identifier is configured using the 'Transcoding ID' parameter (TranscodingID) in the IP Media Settings page (see 'Configuring the IP Media Parameters' on page 399)..

It is assumed that the device is controlled by a third-party, Application server (or any SIP user agent) that instructs the device to start an IP transcoding call by sending two SIP INVITE messages with SIP URI that includes the transcoding identifier name. For example:

```
Invite sip:trans123@audiocodes.com SIP/2.0
```

The left part of the SIP URI includes the transcoding ID (the default string is 'trans') and is terminated by a unique number (123). The device immediately sends a 200 OK message in response to each INVITE.

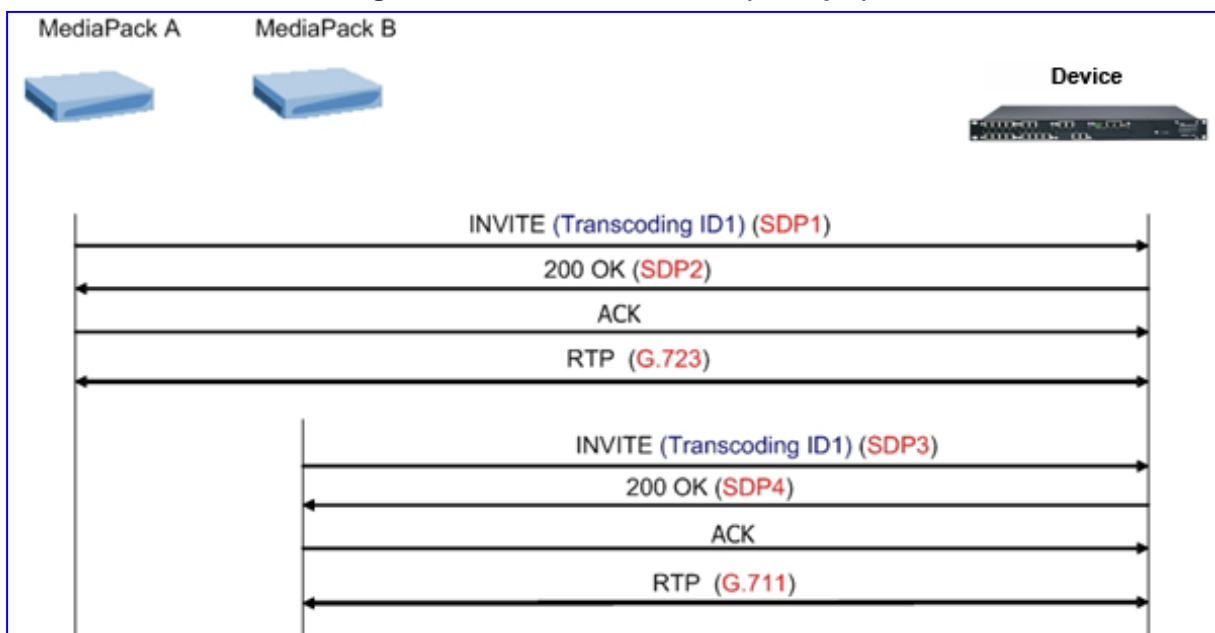
Each of the transcoding SIP call participants can use a different VoIP coder and a different DTMF transport type, negotiated with the device using common SIP negotiation.

Sending a BYE request to the device by any of the participants, terminates the SIP session and removes it from the Transcoding session. The second BYE from the second participant ends the transcoding session and releases its resources.

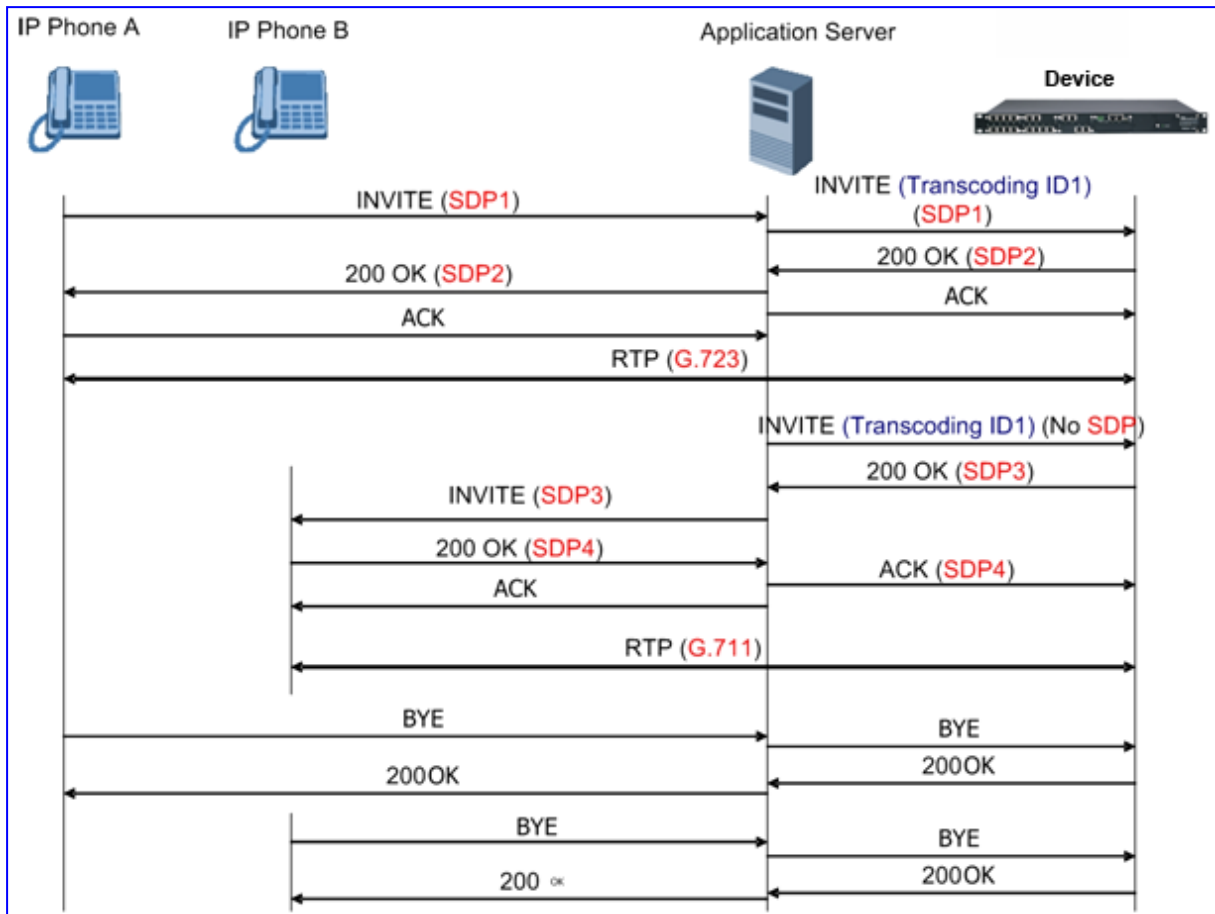
The device uses two media (DSP) channels for each call, thereby reducing the number of available transcoding sessions to half of the defined value for MediaChannels. To limit the number of resources for transcoding, use the 'Number of Media Channels' parameter (MediaChannels) in the IP Media Settings page (see 'Configuring the IP Media Parameters' on page 399). For example, if 'Number of Media Channels' is set to "40", only 20 transcoding sessions are available.

The figure below illustrates an example of a direct connection to a device:

Figure 21-1: Direct Connection (Example)



The figure below illustrates an example of implementing an Application server:



Reader's Notes



Part V

Maintenance

This part describes the maintenance procedures.

Reader's Notes

22 Basic Maintenance

The Maintenance Actions page allows you to perform the following:

- Reset the device - see 'Resetting the Device' on page 467
 - Lock and unlock the device - see 'Locking and Unlocking the Device' on page 469
 - Save configuration to the device's flash memory - see 'Saving Configuration' on page 470
- **To access the Maintenance Actions page, do one of the following:**
- On the toolbar, click the **Device Actions** button, and then from the drop-down menu, choose **Reset**.
 - On the Navigation bar, click the **Maintenance** tab, and then in the Navigation tree, select the **Maintenance** menu and choose **Maintenance Actions**.

Figure 22-1: Maintenance Actions Page

▼ Reset Configuration	
Reset Board	<input type="button" value="Reset"/>
Burn To FLASH	Yes <input type="button" value="v"/>
Graceful Option	No <input type="button" value="v"/>
▼ LOCK / UNLOCK	
Lock	<input type="button" value="LOCK"/>
Graceful Option	No <input type="button" value="v"/>
Current Admin State	UNLOCKED
▼ Save Configuration	
Burn To FLASH	<input type="button" value="BURN"/>

22.1 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).

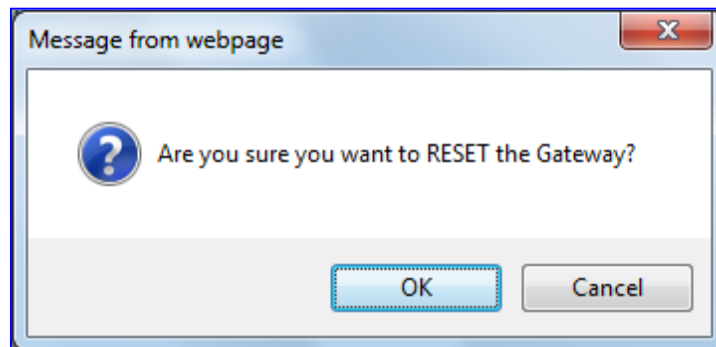


Notes:

- 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 "Reset" (see 'Toolbar' on page 36) to indicate that a device reset is required.
- After you reset the device, the Web GUI is displayed in Basic view (see 'Displaying Navigation Tree in Basic and Full View' on page 38).

- **To reset the device:**
1. Open the Maintenance Actions page (see 'Basic Maintenance' on page 465).
 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 22-2: Reset Confirmation Message Box



6. Click **OK** to confirm device reset; if the parameter 'Graceful Option' is set to **Yes** (in Step 3), the reset is delayed and a screen displaying the number of remaining calls and time is displayed. When the device begins to reset, a message appears notifying you of this.

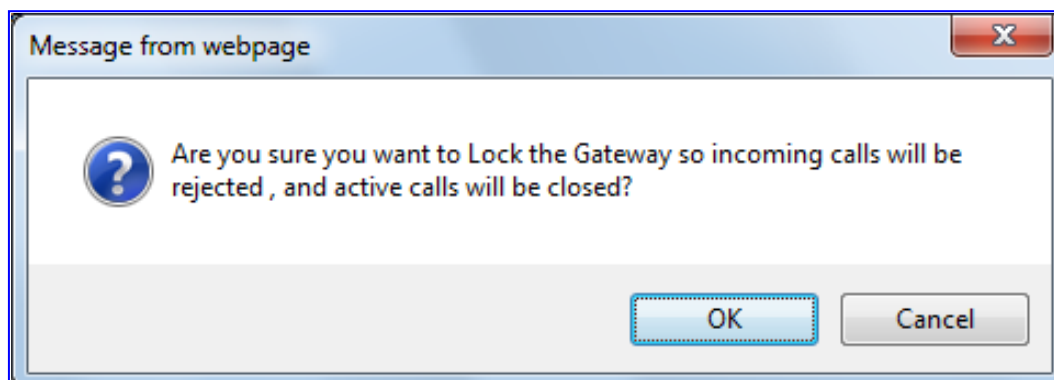
22.2 Locking and Unlocking the Device

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 'Basic Maintenance' on page 465).
 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 22-3: Device Lock Confirmation Message Box



5. Click **OK** to confirm device Lock; if 'Graceful Option' is set to **Yes**, the lock is delayed and a screen displaying the number of remaining calls and time is displayed. Otherwise, the lock process begins immediately. The Current Admin State' field displays the current state - "LOCKED" or "UNLOCKED".

➤ **To unlock the device:**

1. Open the Maintenance Actions page (see 'Maintenance Actions' on page 465).
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 59).

22.3 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 'Basic Maintenance' on page 465).
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 469).
- 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 467).
- The Home page's General Information pane displays whether the device is currently "burning" the configuration (see 'Using the Home Page' on page 59).

23 Software Upgrade

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 471)
- Software Upgrade Key (see 'Loading Software Upgrade Key' on page 485)
- Software Upgrade Wizard (see 'Software Upgrade Wizard' on page 488)
- Configuration File (see 'Backing Up and Loading Configuration File' on page 491)

23.1 Loading Auxiliary Files

Auxiliary files provide the device with additional configuration settings such as call progress tones and prerecorded tones. The table below lists the different types of Auxiliary files:

Table 23-1: Auxiliary Files

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 <i>ini</i> file. For more information on the <i>ini</i> file, see 'INI File-Based Management' on page 83.
CAS	CAS auxiliary files containing the CAS Protocol definitions that are used for CAS-terminated trunks (for various types of CAS signaling). You can use the supplied files or construct your own files. Up to eight different CAS files can be loaded to the device. For more information on CAS files, see CAS Files on page 480.
Voice Prompts	Voice announcement file containing a set of Voice Prompts (VP) that are played by the device during operation. For more information on VP files, see Voice Prompts File on page 479. Note: This file is applicable only to Mediant 1000.
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 more information on the CPT file, see 'Call Progress Tones File' on page 474.
Prerecorded Tones	The Prerecorded Tones (PRT) file enhances the device's capabilities of playing a wide range of telephone exchange tones that cannot be defined in the CPT file. For more information on the PRT file, see 'Prerecorded Tones File' on page 479.
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 more information on the Dial Plan file, see Dial Plan File on page 480.
VXML	Voice Extensible Markup Language (VXML) script file. For more information on VXML, see Voice XML Interpreter on page 438.

File	Description
User Info	The User Information file maps PBX extensions to IP numbers. This file can be used to represent PBX extensions as IP phones in the global 'IP world'. For more information on the User Info file, see 'User Information File' on page 482 .
AMD Sensitivity	Answer Machine Detector (AMD) Sensitivity file containing the AMD Sensitivity suites. For more information on the AMD file, see AMD Sensitivity File on page 483 .

The Auxiliary files can be loaded to the device using one of the following methods:

- Web interface.
- TFTP: This is done by specifying the name of the Auxiliary file in an *ini* file (see Auxiliary and Configuration Files Parameters) and then loading the *ini* file to the device. The Auxiliary files listed in the *ini* file are then automatically loaded through TFTP during device startup. If the *ini* file does not contain a specific auxiliary file type, the device uses the last auxiliary file of that type that was stored on its non-volatile memory.



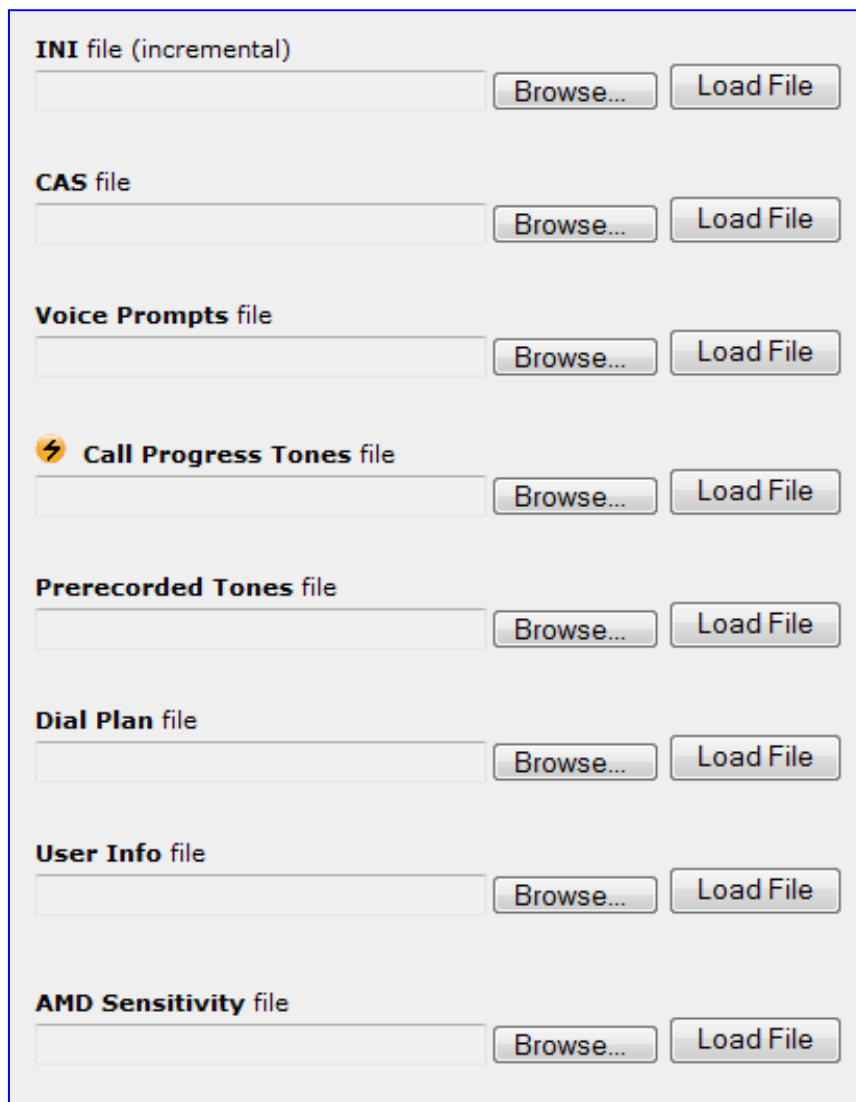
Notes:

- You can schedule automatic loading of updated auxiliary files using HTTP/HTTPS, FTP, or NFS (for more information, refer to the *Product Reference Manual*).
- 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 [469](#)).
- For deleting auxiliary files, see 'Viewing Device Information' on page [497](#).

The procedure below describes how to load Auxiliary files using the Web interface.

➤ **To load auxiliary files to the device using the Web interface:**

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



The screenshot displays a web interface for loading auxiliary files. It features several rows, each with a file type label, an empty text input field, a 'Browse...' button, and a 'Load File' button. The file types listed are: INI file (incremental), CAS file, Voice Prompts file, Call Progress Tones file (marked with a lightning bolt icon), Prerecorded Tones file, Dial Plan file, User Info file, and AMD Sensitivity file.



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 470 and reset the device (if you have loaded a Call Progress Tones file), see 'Resetting the Device' on page 467.

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 762.

➤ **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.

23.1.1 Call Progress Tones File

The Call Progress Tones (CPT) and Distinctive Ringing (applicable to analog interfaces) auxiliary file is comprised of two sections:

- The first section contains the definitions of the Call Progress Tones (levels and frequencies) that are detected/generated by the device.
- The second section contains the characteristics of the Distinctive Ringing signals that are generated by the device (see Distinctive Ringing on page 477).

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
```

23.1.1.1 Distinctive Ringing

Distinctive Ringing is applicable only to FXS interfaces. Using the Distinctive Ringing section of the Call Progress Tones auxiliary file, you can create up to 16 Distinctive Ringing patterns. Each ringing pattern configures the ringing tone frequency and up to four ringing cadences. The same ringing frequency is used for all the ringing pattern cadences. The ringing frequency can be configured in the range of 10 to 200 Hz with a 5 Hz resolution.

Each of the ringing pattern cadences is specified by the following parameters:

- **Burst Ring On Time:** Configures the cadence to be a burst cadence in the entire ringing pattern. The burst relates to On time and the Off time of the same cadence. It must appear between 'First/Second/Third/Fourth' string and the 'Ring On/Off Time'. This cadence rings once during the ringing pattern. Otherwise, the cadence is interpreted as cyclic: it repeats for every ringing cycle.
- **Ring On Time:** Specifies the duration of the ringing signal.
- **Ring Off Time:** Specifies the silence period of the cadence.

The Distinctive Ringing section of the *ini* file format contains the following strings:

- **[NUMBER OF DISTINCTIVE RINGING PATTERNS]:** Contains the following key:
 - 'Number of Distinctive Ringing Patterns' defining the number of Distinctive Ringing signals that are defined in the file.
- **[Ringing Pattern #X]:** Contains the Xth ringing pattern definition (starting from 0 and not exceeding the number of Distinctive Ringing patterns defined in the first section minus 1) using the following keys:
 - **Ring Type:** Must be equal to the Ringing Pattern number.
 - **Freq [Hz]:** Frequency in hertz of the ringing tone.
 - **First (Burst) Ring On Time [10 msec]:** 'Ring On' period (in 10 msec units) for the first cadence on-off cycle.
 - **First (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the first cadence on-off cycle.
 - **Second (Burst) Ring On Time [10 msec]:** 'Ring On' period (in 10 msec units) for the second cadence on-off cycle.
 - **Second (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the second cadence on-off cycle.
 - **Third (Burst) Ring On Time [10 msec]:** 'Ring On' period (in 10 msec units) for the third cadence on-off cycle.
 - **Third (Burst) Ring Off Time [10 msec]:** 'Ring Off' period (in 10 msec units) for the third cadence on-off cycle.
 - **Fourth (Burst) Ring On Time [10 msec]:** 'Ring On' 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
[Ringling 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
[Ringling 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
[Ringling 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
[Ringling 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
```

23.1.2 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 471).

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.

23.1.3 Voice Prompts File

The Voice Prompts (VP) file contains a set of voice prompts (or announcements) that can be played by the device during operation. The voice announcements are prepared offline using standard recording utilities and then combined into a single file using the DConvert utility. The VP file can then be loaded to the device using the BootP/TFTP utility (refer to the *Product Reference Manual*) or Web interface.

The VP file is a collection of raw voice recordings and/or *wav* files. These recordings can be prepared using standard utilities such as CoolEdit and Goldwave™.

The raw data files must be recorded with the following characteristics:

- **Coders:** Linear G.711 A-law or G.711 μ -law
- **Rate:** 8000 kHz
- **Resolution:** 8-bit
- **Channels:** mono

When the list of recorded files is converted to a single *voiceprompts.dat* file, every Voice Prompt is tagged with an ID number, starting with '1'. This ID is later used by the device to play the correct announcement. Up to 1,000 Voice Prompts can be defined. If the size of the combined VP file is less than 1 MB, it can be permanently stored on flash memory.

Larger files (up to 10 MB) are stored in RAM, and should be loaded again (using BootP/TFTP utility) after the device is reset.

The device can be provided with a professionally recorded English (U.S.) VP file.



Note: Voice Prompts are applicable only to Mediant 1000.

- **To generate and load the VP file:**
 1. Prepare one or more voice files using standard utilities.
 2. Use the DConvert utility to generate the *voiceprompts.dat* file from the pre-recorded voice messages (refer to the *Product Reference Manual*).
 3. Load the *voiceprompts.dat* file to the device using TFTP (refer to the Product Reference Manual) or the Web interface (see 'Loading Auxiliary Files' on page 471).

23.1.4 CAS Files

The CAS auxiliary files contain the CAS Protocol definitions that are used for CAS-terminated trunks. You can use the supplied files or construct your own files. Up to eight files can be loaded to the device. Different files can be assigned to different trunks (CAS_{TableIndex_x}) and different CAS tables can be assigned to different B-channels (CAS_{ChannelIndex}).

The CAS files can be loaded to the device using the Web interface or *ini* file (see 'Loading Auxiliary Files' on page 471).



Note: All CAS files loaded together must belong to the same Trunk Type (i.e., either E1 or T1).

23.1.5 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:

- ISDN Overlap Dialing, FXS, and FXO collecting digit mode (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.
- CAS E1 MF-CR2 (Tel-to-IP calls): Useful for E1 MF-CR2 variants that do not support I-15 terminating digits (e.g., in Brazil and Mexico). The Dial Plan file allows the device to detect end-of-dialing in such cases. The *CasTrunkDialPlanName_x* ini file parameter determines which dial plan (in the Dial Plan file) to use for a specific trunk.



Note: To use this Dial Plan, you must also use a special CAS .dat file that supports this feature (contact your AudioCodes sales representative).

- Prefix tags (for IP-to-Tel routing): Provides enhanced routing rules based on Dial Plan

prefix tags. For more information, see Dial Plan Prefix Tags for IP-to-Tel Routing on page 338.

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 471).

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 more information on working with Dial Plan files, see 'External Dial Plan File' on page 335.

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
```

23.1.6 User Information File

The User Information file is a text-based file that can be used for mapping PBX extensions connected to the device to "global" IP numbers.

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 762)
- Web interface (see 'Loading Auxiliary Files' on page 471)
- Automatic update mechanism, using the parameter `UserInfoFileURL` (refer to the *Product Reference Manual*)

23.1.6.1 User Information File for PBX Extensions and "Global" Numbers

The User Information file can be used to map PBX extensions, connected to the device, to global IP numbers. In this context, a global 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 (for analog modules) and 108,000 bytes for digital modules. Each line in the file represents a mapping rule of a single PBX extension. Up to 1,000 rules can be configured. Each line includes five items separated with commas. The items are described in the table below:

Table 23-2: User Information Items

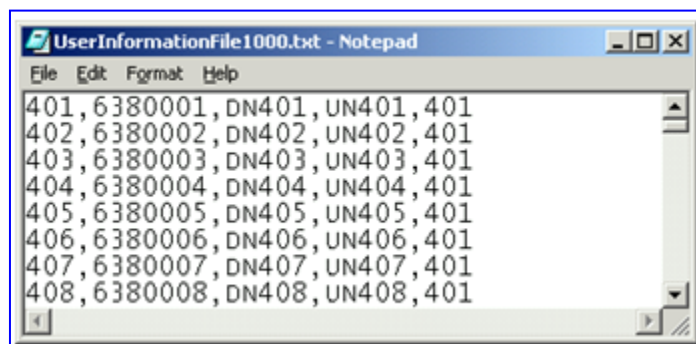
Item	Description	Maximum Size (Characters)
PBX extension #	The relevant PBX extension number.	10
Global phone #	The relevant global phone number.	20
Display name	A string that represents the PBX extensions for the Caller ID.	30
Username	A string that represents the user name for SIP registration.	40
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 23-1: Example of a User Information File



```
UserInformationFile1000.txt - Notepad
File Edit Format Help
401,6380001,DN401,UN401,401
402,6380002,DN402,UN402,401
403,6380003,DN403,UN403,401
404,6380004,DN404,UN404,401
405,6380005,DN405,UN405,401
406,6380006,DN406,UN406,401
407,6380007,DN407,UN407,401
408,6380008,DN408,UN408,401
```



Note: The last line in the User Information file must end with a carriage return (i.e., by pressing the <Enter> key).

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.

23.1.7 AMD Sensitivity File

The AMD Sensitivity file allows you to configure the device with different AMD Sensitivity suites. You can load the device with up to four AMD Sensitivity suites. Each suite can be configured to a different language, country or region, thereby fine tuning the detection algorithm of the DSP according to requirements.

The structure of the file can be viewed in the example below. Each file consists of at least one parameter suite with its suite ID. Each parameter suite consists of up to 16 sensitivity levels, where each level possessing 3 coefficients A, B and C. When loading a new parameter suite, the existing parameter suite with the same ID is overwritten.

The file is created in .xml format and installed on the device as a binary file (with a .dat extension). The XML to binary file format is processed by the DConvert utility (refer to the *Product Reference Manual*).

The file can be installed on the board in the following ways:

- TFTP at initialization time, by setting the *ini* file parameter *AMDSensitivityFileName* with the .dat file name, and adding the file to the TFTP directory.
- Auxiliary files Web page (see 'Loading Auxiliary Files' on page 471).
- Using the AutoUpdate mechanism (refer to the *Product Reference Manual*). In this case the *AMDSensitivityFileUrl* parameter must be set using SNMP or *ini* file.

The following example shows an xml file with two parameter suites:

- Parameter Suite 0 with 6 sensitivity levels,
- Parameter Suite 2 with 3 sensitivity levels.

```

<AMDSENSITIVITY>
<PARAMETERSUIT>
  <PARAMETERSUITID>0</PARAMETERSUITID>
  <!-- First language/country -->
  <NUMBEROFLEVELS>8</NUMBEROFLEVELS>
    <AMDSENSITIVITYLEVEL>
      <!-- Level 0 -->
        <AMDCOEFFICIENTA>15729</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>58163</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>32742</AMDCOEFFICIENTC>
      </AMDSENSITIVITYLEVEL>
    <AMDSENSITIVITYLEVEL>
      <!-- Level 1 -->
        <AMDCOEFFICIENTA>19923</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>50790</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>30720</AMDCOEFFICIENTC>
      </AMDSENSITIVITYLEVEL>
    <AMDSENSITIVITYLEVEL>
      <!-- Level 2 -->
        <AMDCOEFFICIENTA>10486</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>57344</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>25600</AMDCOEFFICIENTC>
      </AMDSENSITIVITYLEVEL>
    <AMDSENSITIVITYLEVEL>
      <!-- Level 3 -->
        <AMDCOEFFICIENTA>8389</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>62259</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>23040</AMDCOEFFICIENTC>
      </AMDSENSITIVITYLEVEL>
    <AMDSENSITIVITYLEVEL>
      <!-- Level 4 -->
        <AMDCOEFFICIENTA>10486</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>50790</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>28160</AMDCOEFFICIENTC>
      </AMDSENSITIVITYLEVEL>
    <AMDSENSITIVITYLEVEL>
      <!-- Level 5 -->
        <AMDCOEFFICIENTA>6291</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>58982</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>23040</AMDCOEFFICIENTC>
      </AMDSENSITIVITYLEVEL>
    <AMDSENSITIVITYLEVEL>
      <!-- Level 6 -->
        <AMDCOEFFICIENTA>7864</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>58982</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>12800</AMDCOEFFICIENTC>
      </AMDSENSITIVITYLEVEL>
  
```

```

    <AMDSENSITIVITYLEVEL>
    <!-- Level 7 -->
        <AMDCOEFFICIENTA>7340</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>64717</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>3840</AMDCOEFFICIENTC>
    </AMDSENSITIVITYLEVEL>
</PARAMETERSUIT>
<PARAMETERSUIT>
    <PARAMETERSUITID>2</PARAMETERSUITID>
    <!-- Second language/country -->
    <NUMBEROFLEVELS>3</NUMBEROFLEVELS>
    <AMDSENSITIVITYLEVEL>
    <!-- Level 0 -->
        <AMDCOEFFICIENTA>15729</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>58163</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>32742</AMDCOEFFICIENTC>
    </AMDSENSITIVITYLEVEL>
    <AMDSENSITIVITYLEVEL>
    <!-- Level 1 -->
        <AMDCOEFFICIENTA>5243</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>9830</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>24320</AMDCOEFFICIENTC>
    </AMDSENSITIVITYLEVEL>
    <AMDSENSITIVITYLEVEL>
    <!-- Level 2 -->
        <AMDCOEFFICIENTA>13107</AMDCOEFFICIENTA>
        <AMDCOEFFICIENTB>61440</AMDCOEFFICIENTB>
        <AMDCOEFFICIENTC>26880</AMDCOEFFICIENTC>
    </AMDSENSITIVITYLEVEL>
</PARAMETERSUIT>
</AMDSENSITIVITY>

```

23.2 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 487)
- AudioCodes' EMS (refer to *EMS User's Manual* or *EMS Product Description*)



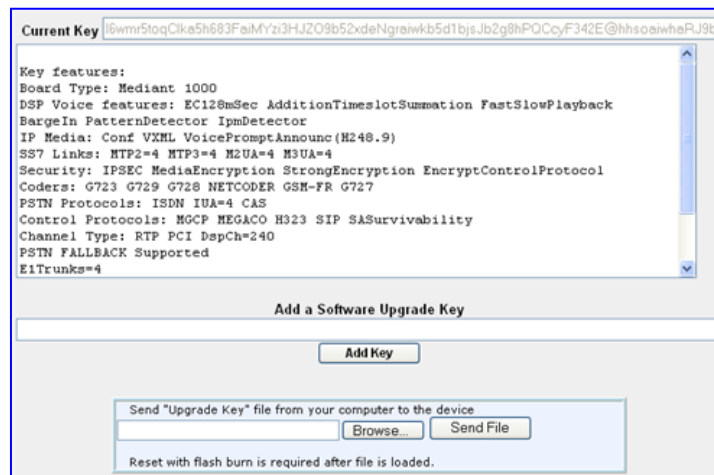
Warning: Do not modify the contents of the Software Upgrade Key file.



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**).



Current Key [6wmf5toqCkIe5h683FaiMYz3HJZO9b52xdeNgraiwb5d1bjsJb2g9hPQCoyF342E@hhsosaiwheRJ9t

Key features:
 Board Type: Mediant 1000
 DSP Voice features: EC128mSec AdditionTimeslotSummation FastSlowPlayback
 BargeIn PatternDetector IpmDetector
 IP Media: Conf VXML VoicePromptAnnounc(H248.9)
 SS7 Links: HTP2=4 HTP3=4 H2UA=4 H3UA=4
 Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
 Coders: G723 G729 G728 NETCODER GSM-FR G727
 PSTN Protocols: ISDN IUA=4 CAS
 Control Protocols: MGCP HEGACO H323 SIP SASurvivability
 Channel Type: RTP PCI DspCh=240
 PSTN FALLBACK Supported
 E1Trunks=4

Add a Software Upgrade Key

Add Key

Send "Upgrade Key" file from your computer to the device

Browse... Send File

Reset with flash burn is required after file is loaded.

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 497).
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 23-2: Software Upgrade Key with Multiple S/N Lines



```

sample.ini - Notepad
File Edit Format Help
[LicenseKeys]
.Board Type 29
S/N241182 =
okRTr5topwYMbIZd4NN2a3Qhm4NjfiDaagUyehso94APbBF85hF4by0cmQZf2B8bMcze7JQ9kMSa5h641R1aOkeEb9AddF894Zx
S/N242519 = tmxTr5to0mlMblZdoPd2a3Qh9zJfida92yehso94PbBF8pi4by0c9paf2B8eOoze7JQgywSa5h6o391aOkeTlAddF8c6Fx
S/N226403 = tmxTr5to0lsMblZdoOB2a3Qh9yJfida92yehso94PbBF8piZ4by0c9ndf2B8eOoze7JQgywSa5h6o2x1aOkeTlAddF8c6Fx
S/N226417 = r6xTr5to25sMblZdfB2a3Qh5OJfida92yehso94PbBF8eOZ4by0c52df2B88yoze7JQInSa5h6tyx1aOkeXZlAddF8amFx
.Board Type 24
S/N241182 =
okRTr5topwYMbIZd4NN2a3wkm4NjfiDaagUyehso94APbBF85hF4by0cmQZf2B8bMcze7JQ9kMSa5h641R1aOkeEb9AddF8938s
S/N242519 = tmxTr5to0mlMblZdoPd2a3wk9zJfida92yehso94PbBF8pi4by0c9paf2B8eOoze7JQgywSa5h6o391aOkeTlAddF8c1ss
S/N226403 = tmxTr5to0lsMblZdoOB2a3wk9yJfida92yehso94PbBF8piZ4by0c9ndf2B8eOoze7JQgywSa5h6o2x1aOkeTlAddF8c1ss
S/N226417 = r6xTr5to25sMblZdfB2a3wk5OJfida92yehso94PbBF8eOZ4by0c52df2B88yoze7JQInSa5h6tyx1aOkeXZlAddF8ahss

```

- In the 'Load 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.
 - Click the **Load 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.
- 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".
 - 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:

- Open the Software Upgrade Key file and check that the S/N line appears. If it does not appear, contact AudioCodes.
- Verify that you've loaded the correct file. Open the file and ensure that the first line displays **[LicenseKeys]**.
- Verify that the content of the file has not been altered.

23.2.1 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 more information on the BootP utility, refer to the *Product Reference Manual*).

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

- Place the Software Upgrade Key file (typically, a .txt file) in the same folder in which the device's *cmp* file is located.
- Start the BootP/TFTP Server utility.
- From the **Services** menu, choose **Clients**; the 'Client Configuration' screen is displayed.
- 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*.

23.3 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 471). However, it is mandatory when using the wizard to first load a *.cmp* file to the device. You can then choose to also load an *ini* file and/or auxiliary files, but this cannot be done without first loading a *.cmp* file. For the *ini* and each auxiliary file type, you can choose to load a new file or not load a file but use the existing file (i.e., maintain existing configuration) running on the device.



Warning: The Software Upgrade Wizard requires the device to be reset at the end of the process, which may disrupt traffic. To avoid this, disable all traffic on the device before initiating the wizard, by performing a graceful lock (see 'Basic Maintenance' on page 465).

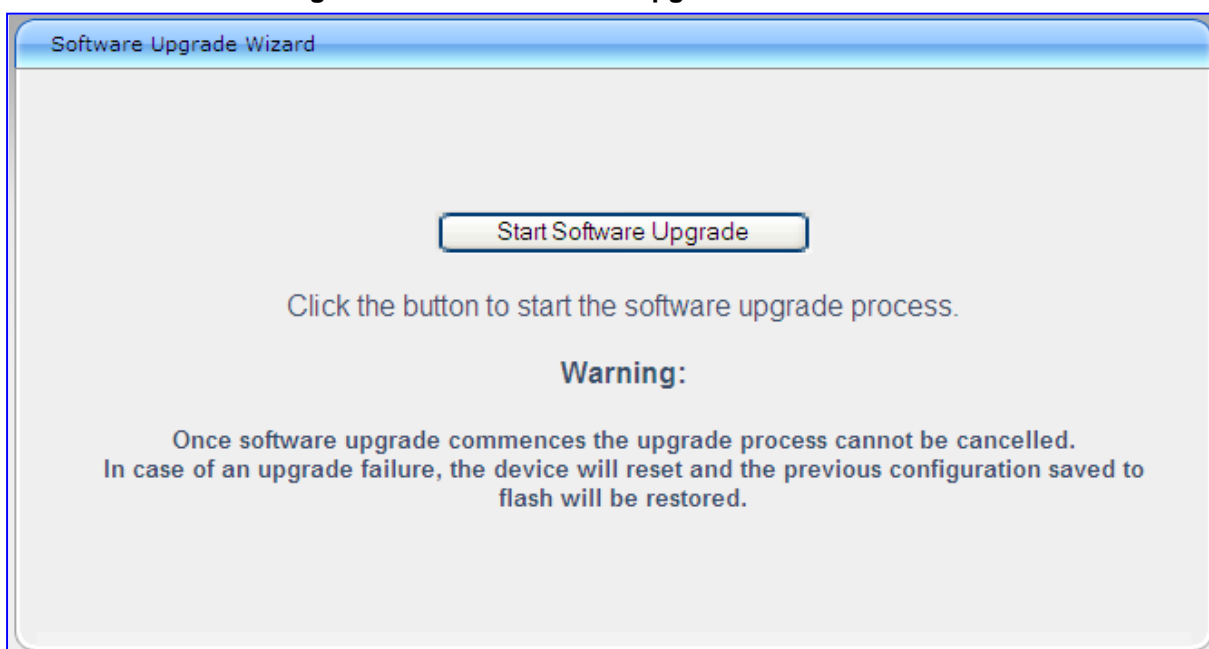
Notes:

- You can get the latest software files from AudioCodes Web site at <http://www.audiocodes.com/downloads>.
- Before upgrading the device, it is recommended that you save a copy of the device's configuration settings (i.e., *ini* file) 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 491.
- 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* file 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, by performing one of the following:
 - Select the **Maintenance** tab, click the **Software Update** menu, and then click **Software Upgrade Wizard**.
 - On the toolbar, click **Device Actions**, and then choose **Software Upgrade Wizard**.


Figure 23-3: Start Software Upgrade Wizard Screen



3. Click the **Start Software Upgrade** button; the wizard starts, requesting you to browse to a .cmp file for uploading.








Note: At this stage, you can quit the Software Update Wizard, by clicking **Cancel** , without requiring a device reset. However, once you start uploading a cmp file, the process must be completed with a device reset. If you choose to quit the process in any of the subsequent pages, the device resets.

4. Click the **Browse** button, navigate to the .cmp file, and then click **Load File**; a progress bar appears displaying the status of the loading process. When the .cmp file is successfully loaded to the device, a message appears notifying you of this.
5. If you want to load **only** a .cmp file, then click the **Reset**  button to reset the device with the newly loaded .cmp file, utilizing the existing configuration (*ini*) and auxiliary files. To load additional files, skip to Step 7.



Note: Device reset may take a few minutes depending on cmp file version (this may even take up to 10 minutes).

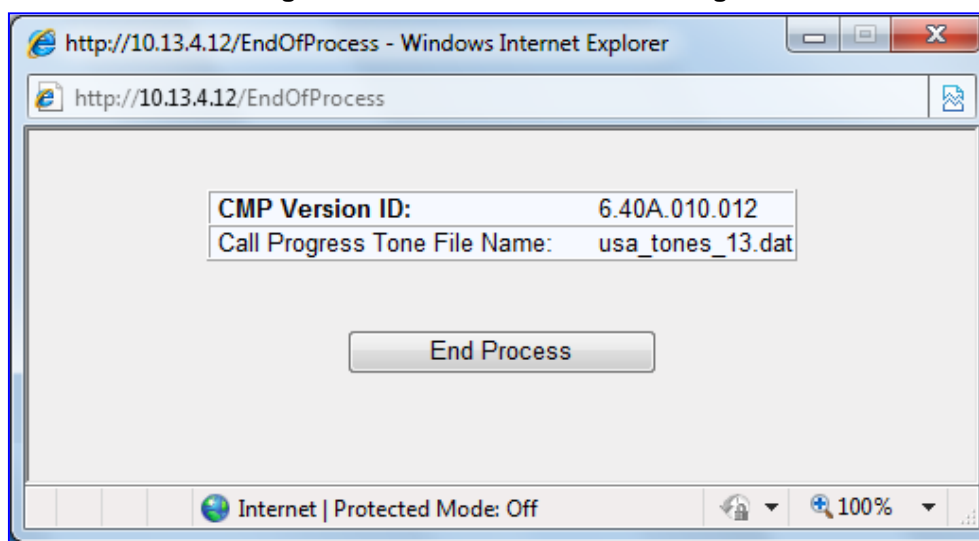
6. Click the **Next**  button; the wizard page for loading an *ini* file appears. You can now perform one of the following:
 - Load a new *ini* file: Click **Browse**, navigate to the *ini* file, and then click **Send File**; the *ini* file is loaded to the device and you're notified as to a successful 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 of Process wizard page appears displaying the new .cmp and auxiliary files loaded to the device.

Figure 23-4: 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.

23.4 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 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**.

Configuration File

Save the **INI** file to the PC.

Save INI File

Load the **INI** file to the device.

Browse... Load INI File

The device will perform a reset after loading the **INI** file.

2. Click the **Save INI File** button; the 'File Download' dialog box appears.
3. 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.

- **To load the ini file:**
1. 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.
 2. Click the **Load INI File** button, and then at the prompt, click **OK**; the device uploads the *ini* file and then resets (from the *cmp* version stored on the flash memory). Once complete, the Login screen appears, requesting you to enter your user name and password.

24 Restoring Factory Defaults

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 493)
- Using the hardware Reset button (see Restoring Defaults using Hardware Reset Button on page 494)
- Loading an empty *ini* file (see 'Restoring Defaults using an ini File' on page 494)

24.1 Restoring Defaults using CLI

The device can be restored to factory defaults using CLI, as described in the procedure below.

➤ **To restore factory defaults using CLI:**

1. Access the CLI:
 - a. Connect the RS-232 serial port of the device to the communication port on your PC. For cabling the device, refer to the *Hardware Installation Manual*.
 - b. Establish serial communication with the device using a serial communication program (such as HyperTerminal™) with the following communication port settings:
 - ◆ **Baud Rate:** 115,200 bps
 - ◆ **Data Bits:** 8
 - ◆ **Parity:** None
 - ◆ **Stop Bits:** 1
 - ◆ **Flow Control:** None
2. At the CLI prompt, type the following command to access the configuration mode, and then press Enter:

```
conf
```
3. At the prompt, type the following command to reset the device to default settings, and then press Enter:

```
RestoreFactorySettings
```

24.2 Restoring Defaults using Hardware Reset Button

The device's hardware Reset pinhole button can be used to reset the device to default settings.

➤ **To restore default settings using the hardware Reset button:**

- With a paper clip or any other similar pointed object, press and hold down the Reset button (located on the CPU module) for at least 12 seconds (but no more than 25 seconds).

24.3 Restoring Defaults using an ini File

You can restore the device to factory default settings by loading an empty *ini* file to the device, using the Web interface's Configuration File page (see 'Backing Up and Loading Configuration File' on page 491). 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.



Part VI

Status, Performance Monitoring and Reporting

This part describes the status and performance monitoring procedures.

Reader's Notes

25 System Status

This section describes how to view system status.

- Syslog messages - see Viewing Syslog Messages on page 527
- Device information - see 'Viewing Device Information' on page 497
- Ethernet port information - see 'Viewing Ethernet Port Information' on page 498

25.1 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**).

▼ General Settings	
MAC Address:	00908f222e30
Serial Number:	2240048
Board Type:	Mediant 1000
Device Up Time:	0d:0h:31m:15s:20th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size [bytes]:	64
RAM Size [bytes]:	268435456
CPU Speed [MHz]:	500
▼ Versions	
Version ID:	6.40A.010.012
DSP Type:	2
DSP Software Version:	60007
DSP Software Name:	624AE3
Flash Version:	520
▼ Loaded Files	
Call Progress Tones File Name:	usa_tones_13.dat <input type="button" value="Delete"/>
Loaded Coder Table :	Default CODERTABLE

➤ **To delete a loaded file:**

- Click the **Delete** button corresponding to the file that you want to delete. Deleting a file takes effect only after device reset (see 'Resetting the Device' on page 467).

25.2 Viewing Ethernet Port Information

The Ethernet Port Information page displays read-only information on the Ethernet port connections. This includes information such as activity status, duplex mode, and speed.



Notes:

- The Ethernet Port Information page can also be accessed from the Home page (see 'Using the Home Page' on page 59).
- For information on the Ethernet redundancy scheme, see Ethernet Interface Redundancy.

➤ To view Ethernet port information:

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

Ethernet Information	
Active Port	1
Port 1 Duplex Mode	Half Duplex
Port 1 Speed	100 Mbps
Port 2 Duplex Mode	Not Available
Port 2 Speed	Not Available

Table 25-1: Ethernet Port Information Parameters

Parameter	Description
Active Port	Displays the active Ethernet port (1 or 2).
Port Duplex Mode	Displays the Duplex mode of the Ethernet port.
Port Speed	Displays the speed (in Mbps) of the Ethernet port.

26 Carrier-Grade Alarms

This section describes how to view the following types of alarms:

- Active alarms - see 'Viewing Active Alarms' on page 499
- Alarm history - see 'Viewing Alarm History' on page 500

26.1 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 59).

➤ **To view the list of active alarms:**

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

Sequential number	Severity	Source	Description	Date
1	Major	Board#1/WanLink#1	WAN link alarm. FE interface 1 is down.	25.8.2011 , 16:28:47
2	Minor	Board#1/EthernetLink#2	Ethernet link alarm. LAN port number 2 is down.	25.8.2011 , 16:28:47
3	Minor	Board#1/EthernetLink#3	Ethernet link alarm. LAN port number 3 is down.	25.8.2011 , 16:28:47

For each alarm, the following information is provided:

- **Severity:** severity level of the alarm:
 - Critical (red)
 - Major (orange)
 - Minor (yellow)
- **Source:** unit from which the alarm was raised
- **Description:** brief explanation of the alarm
- **Date:** date and time that the alarm was generated

You can view the next 20 alarms (if exist), by clicking the **Go to page** button.

26.2 Viewing Alarm History

The Alarms History page displays a list of alarms that have been raised and traps that have been cleared.

➤ **To view the list of history alarms:**

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

Sequential number	Severity	Source	Description	Date
1	Major	Board#1	Controller failure alarm Proxy Set 0: Proxy lost, looking for another proxy	6.1.2010 , 14:1:26
2	Cleared	Board#1	Alarm cleared: Controller failure alarm Proxy Set 0: Proxy lost, looking for another proxy	6.1.2010 , 14:1:26
3	Major	Board#1	Controller failure alarm Proxy Set ID 0	6.1.2010 , 14:1:26
4	Major	Board#1/WanLink#1	WAN link alarm. FE interface 1 is down.	6.1.2010 , 14:1:29
5	Minor	Board#1/EthernetLink#2	Ethernet link alarm. LAN port number 2 is down.	6.1.2010 , 14:1:29
6	Major	Board#1	NTP server alarm. No connection to NTP server.	6.1.2010 , 14:11:14

For each alarm, the following information is provided:

- **Severity:** severity level of the alarm:
 - Critical (red)
 - Major (orange)
 - Minor (yellow)
 - Cleared (green)
- **Source:** unit from which the alarm was raised
- **Description:** brief explanation of the alarm
- **Date:** date and time that the alarm was generated

You can view the next 20 alarms (if exist), by clicking the **Go to page** button.

27 Performance Monitoring

This section describes how to view the following performance monitoring graphs:

- Trunk Utilization - see 'Viewing Trunk Utilization' on page 501
- MOS per Media Realm - see 'Viewing MOS per Media Realm' on page 503

27.1 Viewing Trunk Utilization

The Trunk Utilization page provides an X-Y graph that displays the number of active channels per trunk over time. The x-axis indicates the time; the y-axis indicates the number of active trunk channels.

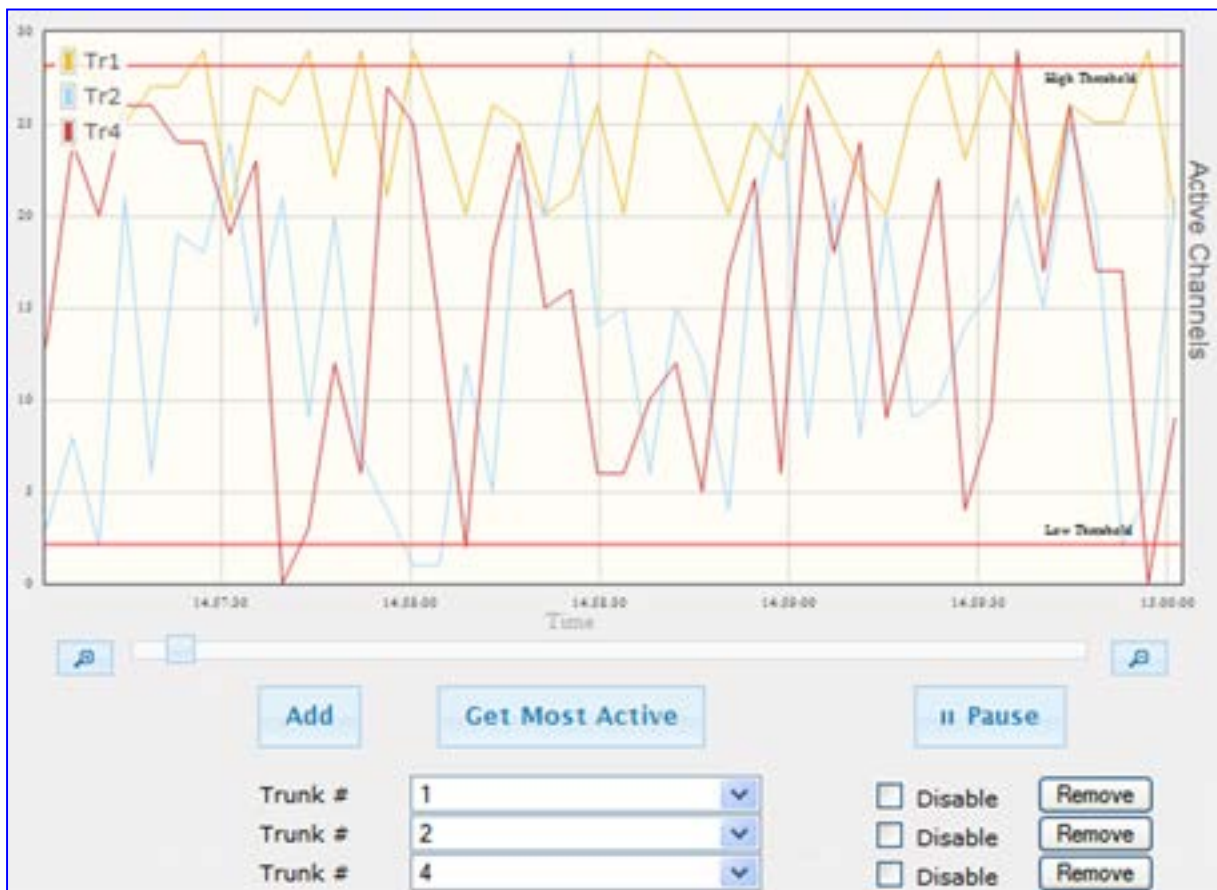


Note: If you navigate to a different page, the data displayed in the graph and all its settings are cleared.

➤ **To view the number of active trunk channels**

1. Open the Trunk Utilization page (**Status & Diagnostics** tab > **Performance Monitoring** menu > **Trunk Utilization**).



Figure 27-1: Trunk Utilization Page



2. From the 'Trunk' drop-down list, select the trunk for which you want to view active channels.

For more graph functionality, see the following table:

Table 27-1: Additional Graph Functionality for Trunk Utilization

Button	Description
Add button	Displays additional trunks in the graph. Up to five trunks can be displayed simultaneously in the graph. To view another trunk, click this button and then from the new 'Trunk' drop-down list, select the required trunk. Each trunk is displayed in a different color, according to the legend shown in the top-left corner of the graph.
Remove button	Removes the selected trunk display from the graph.
Disable check box	Hides or shows an already selected trunk. Select this check box to temporarily hide the trunk display; clear this check box to show the trunk. This is useful if you do not want to remove the trunk entirely (using the Remove button).
Get Most Active button	Displays only the trunk with the most active channels (i.e., trunk with the most calls).
Pause button	Pauses the display in the graph.
Play button	Resumes the display in the graph.
Zoom slide ruler and buttons	Increases or reduces the trunk utilization display resolution concerning time. The Zoom In  button increases the time resolution; the Zoom Out  button decreases it. Instead of using the buttons, you can use the slide ruler. As you increase the resolution, more data is displayed on the graph. The minimum resolution is about 30 seconds; the maximum resolution is about an hour.

27.2 Viewing MOS per Media Realm

The MOS Per Media Realm page displays statistics on Media Realms (configured in 'Configuring Media Realms' on page 170). This page provides two graphs:

- Upper graph: displays the Mean Opinion Score (MOS) quality in RTCP data per selected Media Realm.
- Lower graph: displays the bandwidth of transmitted media (in Kbps) in RTCP data per Media Realm.



➤ **To view the MOS per Media Realm graph:**

1. Open the MOS Per Media Realm page (**Status & Diagnostics** tab > **Performance Monitoring** menu > **MOS Per Media Realm**).

Figure 27-2: MOS Per Media Realm Graph



2. From the 'Media Realm' drop-down list, select the Media Realm for which you want to view.

Use the **Zoom In**  button to increase the displayed time resolution or the **Zoom Out**  button to decrease it. Instead of using these zoom buttons, you can use the slide ruler. As you increase the resolution, more data is displayed on the graph. The minimum resolution is about 30 seconds; the maximum resolution is about an hour.

To pause the graph, click the **Pause** button; click **Play** to resume.

Reader's Notes

28 VoIP Status

This section describes how to view the following VoIP status and statistics:

- IP network interface - see 'Viewing Active IP Interfaces' on page 505
- Performance - see 'Viewing Performance Statistics' on page 505
- IP-to-Tel calls - see 'Viewing Call Counters' on page 506
- Tel-to-IP calls - see 'Viewing Call Counters' on page 506
- SAS registered users - see Viewing SAS/SBC Registered Users on page 508
- Call routing - see 'Viewing Call Routing Status' on page 508
- Registration - see Viewing Registration Status on page 509
- IP connectivity - see 'Viewing IP Connectivity' on page 510

28.1 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 102).

➤ **To view the Active IP Interfaces page:**

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

Index	Application Type	Address Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
NA	O+M+C	IPv4	IPv4 Manual	10.13.4.13	16	10.13.0.1	0	O+M+C

VLAN Mode	Disabled
Native VLAN ID	1

28.2 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 28-1: Basic Statistics Page

(Statistics for 251040 seconds)	
Active TDM channels	0
Active DSP resources	0
Active analog channels	0
Active G.711 channels	0
Average voice delay (ms)	0
Average voice jitter (ms)	0
Total RTP packets TX	0
Total RTP packets RX	0
Total call attempts	0

To reset the performance statistics to zero, click the **Reset Statistics** button.

28.3 Viewing Call Counters

The IP to Tel Calls Count page and Tel to IP Calls Count page provide you with statistical information on incoming (IP-to-Tel) and outgoing (Tel-to-IP) calls. The statistical information is updated according to the release reason that is received after a call is terminated (during the same time as the end-of-call Call Detail Record or CDR message is sent). The release reason can be viewed in the 'Termination Reason' field in the CDR message.

You can reset the statistical data displayed on the page (i.e., refresh the display), by clicking the **Reset Counters** button located 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 28-2: Calls Count Page

▼	
Number of Attempted Calls	19
Number of Established Calls	14
Percentage of Successful Calls(ASR)	73.684211
Number of Calls Terminated due to a Busy Line	2
Number of Calls Terminated due to No Answer	0
Number of Calls Terminated due to Forward	0
Number of Failed Calls due to No Route	0
Number of Failed Calls due to No Matched Capabilities	0
Number of Failed Calls due to No Resources	0
Number of Failed Calls due to Other Failures	0
Average Call Duration(ACD)[sec]	25
Attempted Fax Calls Counter	0
Successful Fax Calls Counter	0

The fields in this page are described in the following table:

Table 28-1: 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	<p>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:</p> <ul style="list-style-type: none"> ▪ GWAPP_REASON_NOT_RELEVANT (0) ▪ GWAPP_NORMAL_CALL_CLEAR (16) ▪ GWAPP_NORMAL_UNSPECIFIED (31) <p>And the internal reasons:</p> <ul style="list-style-type: none"> ▪ RELEASE_BECAUSE_UNKNOWN_REASON ▪ RELEASE_BECAUSE_REMOTE_CANCEL_CALL ▪ RELEASE_BECAUSE_MANUAL_DISC ▪ RELEASE_BECAUSE_SILENCE_DISC ▪ RELEASE_BECAUSE_DISCONNECT_CODE <p>Note: When the duration of the call is zero, the release reason GWAPP_NORMAL_CALL_CLEAR increments the 'Number of Failed</p>

Counter	Description
	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: <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ▪ 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.

28.4 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 registered users:**

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

Figure 28-3: SAS/SBC Registered Users Page

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

Table 28-2: 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.

28.5 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 28-4: Call Routing Status Page

Call-Routing Method		Proxy/GK
▼ Active Proxy Sets Status		
ID	IP Address	State
0	-- (--)	--
1	-- (--)	--
2	-- (--)	--
3	-- (--)	--
4	10.13.4.6 (10.13.4.6)	OK
5	-- (--)	--
6	-- (--)	--
7	-- (--)	--
8	-- (--)	--
9	-- (--)	--

Table 28-3: Call Routing Status Parameters

Parameter	Description
Call-Routing Method	<ul style="list-style-type: none"> Proxy/GK = Proxy server is used to route calls. Routing Table = The Outbound IP Routing Table is used to route calls.
IP Address	<ul style="list-style-type: none"> Not Used = Proxy server isn't defined. IP address and FQDN (if exists) of the Proxy server with which the device currently operates.
State	<ul style="list-style-type: none"> 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.

28.6 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 28-5: Registration Status Page

Registered Per Gateway		NO	
▼ Ports Registration Status			
Gateway Port		Status	
Module 3	Port 1 FXS	NOT REGISTERED	
Module 3	Port 2 FXS	NOT REGISTERED	
Module 3	Port 3 FXS	NOT REGISTERED	
Module 3	Port 4 FXS	NOT REGISTERED	
▼ Accounts Registration Status			
Index	Group Type	Group Name	Status
▼ BRI Phone Numbers Status			
Phone Number	Module / Port	Status	

- **Registered Per Gateway:**
 - "YES" = registration is per device
 - "NO" = registration is not per device
- **Ports Registration Status:**
 - "REGISTERED" = channel is registered
 - "NOT REGISTERED" = channel not registered
- **Accounts Registration Status:** registration status based on the Accounts table (configured in 'Configuring Account Table' on page 223):
 - **Group Type:** type of served group - Trunk Group or IP Group

- **Group Name:** name of the served group, if applicable
- **Status:** indicates whether or not the group is registered ("Registered" or "Unregistered")
- **BRI Phone Number Status:**
 - Phone Number: phone number of BRI endpoint
 - Module/Port: module/port number of BRI endpoint
 - Status: indicates whether or not the BRI endpoint is registered ("Registered" or "Unregistered")



Note: The registration mode (i.e., per device, endpoint, account. or no registration) is configured in the Trunk Group Settings table (see 'Configuring Trunk Group Settings' on page 251) or using the TrunkGroupSettings *ini* file parameter.

28.7 Viewing IP Connectivity

The IP Connectivity page displays online, read-only network diagnostic connectivity information on all destination IP addresses configured in the Outbound IP Routing Table page (see 'Configuring Outbound IP Routing Table' on page 269).



Notes:

- This information is available only if the parameter 'Enable Alt Routing Tel to IP'/AltRoutingTel2IPMode (see 'Configuring General Routing Parameters' on page 268) 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 'Enable Alt Routing Tel to IP' parameter (AltRoutingTel2IPEnable) to **Enable** or **Status Only**.
 2. Open the IP Connectivity page (**Status & Diagnostics** tab > **VoIP Status** menu > **IP Connectivity**).

Figure 28-6: 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 28-4: IP Connectivity Parameters

Column Name	Description
IP Address	The IP address can be one of the following: <ul style="list-style-type: none"> IP address defined as the destination IP address in the Outbound IP Routing Table'. IP address resolved from the host name defined as the destination IP address in the Outbound IP Routing Table'.
Host Name	Host name (or IP address) as defined in the Outbound IP Routing Table'.
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. <ul style="list-style-type: none"> 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 <i>ini</i>) is set to 'None' or 'QoS'.
Quality Status	Determines the QoS (according to packet loss and delay) of the IP address. <ul style="list-style-type: none"> Unknown = Recent quality information isn't available. OK Poor Notes: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> DNS Disable DNS Resolved DNS Unresolved

Reader's Notes

29 Reporting Information to External Party

29.1 Generating Call Detail Records

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 517.

29.1.1 CDR Fields for Gateway Application

The CDR fields for the Gateway (and IP-to-IP) applications are listed in the table below.

Table 29-1: CDR Fields for Gateway/IP2IP Application

Field Name	Description
ReportType	Report type (call started, call connected, or call released)
Cid	Port number
SessionId	SIP session identifier
Trunk	Physical trunk number
BChan	Selected B-channel
ConId	SIP conference ID
TG	Trunk Group ID
EPTyp	Endpoint type (FXS or FXO)
Orig	Call originator (IP or Tel)
Sourcelp	Source IP address
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
Rtplp	RTP IP address
Port	Remote RTP port

Field Name	Description
TrmSd	Initiator of call release (IP, Tel, or Unknown)
TrmReason	Termination reason (see 'Release Reasons in CDR' on page 515)
Fax	Fax transaction during call
InPackets	Number of incoming packets
OutPackets	Number of outgoing packets
PackLoss	Local packet loss
RemotePackLoss	Number of outgoing lost packets
SIPCallId	Unique SIP call 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
NPI	Redirection phone number plan
RedirectPhonNum	Redirection phone number
MeteringPulses	Number of generated metering pulses
SrcHost	Source host name
SrcHostBeforeMap	Source host name before manipulation
DstHost	Destination host name
DstHostBeforeMap	Destination host name before manipulation
IPG	IP Group description
LocalRtplp	Remote RTP IP address
LocalRtpPort	Local RTP port
TrmReasonCategory	Termination reason category
RedirectNumBeforeMap	Redirect number before manipulation
SrdId	SRD ID
SIPInterfaceld	SIP interface ID
TransportType	SIP transport type (UDP, TCP, or TLS)
TxRTPIPDiffServ	Media IP DiffServ
TxSigIPDiffServ	Signaling IP DiffServ
LocalRFactor	Local R-factor

Field Name	Description
RemoteRFactor	Remote R-factor
LocalMosCQ	Local MOS for conversation quality
RemoteMosCQ	Remote MOS for conversation quality
SourcePort	Source RTP port
DestPort	Destination RTP port

29.1.2 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_UNKNOWN_ERROR"
- "RELEASE_BECAUSE_HELD_TIMEOUT"

29.1.3 Supported RADIUS Attributes

The following table provides descriptions on the RADIUS attributes included in the communication packets transmitted between the device and a RADIUS Server.

Table 29-2: 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-	25	Setup time in NTP format	String		Start Acc

Attribute Number	Attribute Name	VSA No.	Purpose	Value Format	Example	AAA'
	Time		1			Stop Acc
26	H323-Call-Origin	26	The call's originator: Answering (IP) or Originator (PSTN)	String	Answer, Originate etc	Start Acc Stop Acc
26	H323-Call-Type	27	Protocol type or family used on this leg of the call	String	VoIP	Start Acc Stop Acc
26	H323-Connect-Time	28	Connect time in NTP format	String		Stop Acc
26	H323-Disconnect-Time	29	Disconnect time in NTP format	String		Stop Acc
26	H323-Disconnect-Cause	30	Q.931 disconnect cause code	Numeric		Stop Acc
26	H323-Gw-ID	33	Name of the gateway	String	SIPIDString	Start Acc Stop Acc
26	SIP-Call-ID	34	SIP Call ID	String	abcde@ac.com	Start Acc Stop Acc
26	Call-Terminator	35	The call's terminator: PSTN-terminated call (Yes); IP-terminated call (No).	String	Yes, No	Stop Acc
30	Called-Station-ID			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

Attribute Number	Attribute Name	VSA No.	Purpose	Value Format	Example	AAA ¹
			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
```

29.2 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 29-3: Supported X-Detect Event Types

Events Type	Subtype	Required Configuration
AMD	voice automatic silence unknown beep	EnableDSPIPMDetectors = 1 AMDTimeout = 2000 (msec) For AMD beep detection, AMDBeepDetectionMode = 1 or 2
CPT	SIT-NC SIT-IC SIT-VC SIT-RO Busy Reorder Ringtone beep	SITDetectorEnable = 1 UserDefinedToneDetectorEnable = 1 Notes: <ul style="list-style-type: none"> ▪ 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 29-4: 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).
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 = [AMD | 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
    
```

29.3 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 specifies the total and the free number of channels associated with media services (e.g., announcements and conferencing)

Below is an example of the X-Resources:

```
X-Resources: telchs= 12/4;mediachs=0/0
```

In the example above, "telchs" specifies the number of available channels and the number of occupied channels (4 channels are occupied and 12 channels are available).



Part VII

Diagnostics

This part describes the diagnostics procedures.

Reader's Notes


30 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 551. For viewing Syslog messages in the Web interface, see Viewing Syslog Messages on page 527. For more information 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 30-1: Syslog Settings Page

▼ Syslog Settings	
Enable Syslog	Disable <input type="button" value="v"/>
Syslog Server IP Address	<input type="text"/>
Syslog Server Port	514 <input type="text"/>
Debug Level	0 <input type="button" value="v"/>
Analog Ports Filter	-1 <input type="text"/>
Trunks Ports Filter	-1 <input type="text"/>
▼ Activity Types to Report via 'Activity Log' Messages	
Parameters Value Change	<input type="checkbox"/>
Auxiliary Files Loading	<input type="checkbox"/>
 Device Reset	<input type="checkbox"/>
Flash Memory Burning	<input type="checkbox"/>
Device Software Update	<input type="checkbox"/>
Access to Restricted Domains	<input type="checkbox"/>
Non-Authorized Access	<input type="checkbox"/>
Sensitive Parameters Value Change	<input type="checkbox"/>
Login and Logout	<input type="checkbox"/>

2. Configure the parameters as required, and then click **Submit** to apply your changes.
3. To save the changes to flash memory, see 'Saving Configuration' on page 470.

Reader's Notes

31 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 525).
- 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 31-1: Message Log Page

```
Log is Activated

11d:14h:43m:9s ( lgr_psrbdex) (2662 ) recv <-- ON_HOOK Ch:1
11d:14h:43m:9s ( lgr_flow) (2663 ) #1:ON_HOOK_EV
11d:14h:43m:9s ( lgr_flow) (2664 ) | #1:ON_HOOK_EV
11d:14h:43m:9s ( lgr_psrbdif) (2665 ) #1:cpDigitMapHndlr_Stop - Stopped (0)
11d:14h:43m:9s ( lgr_psrbdif) (2666 ) #1:CloseChannel: ChannelNum=1
11d:14h:43m:9s ( lgr_psrbdif) (2667 ) Open channel: IsVoiceOn: 1, IsT38On: 1, IsVbdOn: 0, Is
11d:14h:43m:9s ( lgr_psrbdif) (2668 ) #1:OpenChannel:on Trunk -1 BChannel:1 CID=1 with Voice
11d:14h:43m:9s ( lgr_psrbdif) (2669 ) #1:OpenChannel VoiceVolume= 0, DTHFVolume = -11, Input
11d:14h:43m:9s ( lgr_psrbdif) (2670 ) OpenChannel, CoderType = 15, Interval = 4, M = 1
11d:14h:43m:9s ( lgr_psrbdif) (2671 ) #1:FAXtransportType = 1
11d:14h:43m:9s ( lgr_psrbdif) (2672 ) #1:ConfigFaxModemChannelParams NSEMode=0, CNGDetMode=
11d:14h:43m:9s ( lgr_psrbdif) (2673 ) Detectors: Amd:0, Ans:0 En:0 IBScmd:Oxal
11d:14h:43m:9s ( lgr_psrbdif) (2674 ) #1:PSOSBoardInterface::StopPlayTone- Called
11d:14h:43m:9s ( lgr_psrbdex) (2675 ) recv <-- OFF_HOOK Ch:1
11d:14h:43m:9s ( lgr_flow) (2676 ) #1:OFF_HOOK_EV
11d:14h:43m:9s ( lgr_flow) (2677 ) | #1:OFF_HOOK_EV
11d:14h:43m:9s ( lgr_psrbdif) (2678 ) UpdateChannelParams, Channel 1
11d:14h:43m:9s ( lgr_psrbdif) (2679 ) #1:ConfigFaxModemChannelParams NSEMode=0, CNGDetMode=
11d:14h:43m:9s ( lgr_psrbdif) (2680 ) ActivatedDigitMap for channel : 1, MaxDialStringLength
```

The displayed logged messages are color coded as follows:

- Yellow - fatal error message
 - Blue - recoverable error message (i.e., non-fatal error)
 - Black - notice message
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.

Reader's Notes



Part VIII

Appendices

This part includes various appendices.

Reader's Notes

A 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.

A.1 Networking Parameters

This subsection describes the device's networking parameters.

A.1.1 Ethernet Parameters

The Ethernet parameters are described in the table below.

Table A-1: Ethernet Parameters

Parameter	Description
EMS: Physical Configuration [EthernetPhyConfiguration]	<p>Defines the Ethernet connection mode type.</p> <ul style="list-style-type: none"> ▪ [0] = 10Base-T half-duplex ▪ [1] = 10Base-T full-duplex ▪ [2] = 100Base-TX half-duplex ▪ [3] = 100Base-TX full-duplex ▪ [4] = Auto-negotiate (default) <p>Note: For this parameter to take effect, a device reset is required.</p>
[MIIRedundancyEnable]	<p>Enables the Ethernet Interface Redundancy feature. When enabled, the device performs a switchover to the second (redundant) Ethernet port upon sensing a link failure in the primary Ethernet port. When disabled, the device operates with a single port (i.e. no redundancy support).</p> <ul style="list-style-type: none"> ▪ [0] = Disable ▪ [1] = Enable (default) <p>For more information on Ethernet interface redundancy, see Ethernet Interface Redundancy on page 102.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>

A.1.2 Multiple Network Interfaces and VLAN Parameters

The IP network interfaces and VLAN parameters are described in the table below.

Table A-2: IP Network Interfaces and VLAN Parameters

Parameter	Description
Multiple Interface Table	
Web: Multiple Interface Table EMS: IP Interface Settings [InterfaceTable]	<p>This <i>parameter</i> table configures the Multiple Interface table for configuring logical IP addresses. The format of this parameter is as follows:</p> <pre>[InterfaceTable] FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID, InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress, InterfaceTable_SecondaryDNSServerIPAddress, InterfaceTable_UnderlyingInterface; [InterfaceTable]</pre> <p>For example: InterfaceTable 0 = 0, 0, 192.168.85.14, 16, 0.0.0.0, 1, Management; InterfaceTable 1 = 2, 0, 200.200.85.14, 24, 0.0.0.0, 200, Control; InterfaceTable 2 = 1, 0, 211.211.85.14, 24, 211.211.85.1, 211, Media;</p> <p>The above example, configures three network interfaces (OAMP, Control, and Media).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this <i>parameter</i> table to take effect, a device reset is required. ▪ Up to 16 logical IP addresses with associated VLANs can be defined (indices 0-15). ▪ Each interface index must be unique. ▪ 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.

Parameter	Description
	<ul style="list-style-type: none"> 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 102). For a description of configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Single IP Network Parameters	
Web: IP Address EMS: Local IP Address [LocalOAMIPAddress]	<p>Defines 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.</p> <p>The default value is 0.0.0.0.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: Subnet Mask EMS: OAM Subnet Mask [LocalOAMSubnetMask]	<p>Defines the device's subnet mask of the OAMP interface when operating in a single interface scenario without a Multiple Interface table.</p> <p>The default subnet mask is 0.0.0.0.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: Default Gateway Address EMS: Local Def GW [LocalOAMDefaultGW]	<p>Defines the Default Gateway of the OAMP interface when operating in a single interface scenario without a Multiple Interface table.</p>
VLAN Parameters	
Web/EMS: VLAN Mode [VLANMode]	<p>Enables the VLAN functionality.</p> <ul style="list-style-type: none"> [0] Disable (default). [1] Enable = VLAN tagging (IEEE 802.1Q) is enabled. <p>Notes:</p> <ul style="list-style-type: none"> 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 unavailable.
Web/EMS: Native VLAN ID [VLANNativeVLANID]	<p>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).</p> <p>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).</p> <p>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.</p> <p>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</p>

Parameter	Description
	parameter to a value other than any VLAN ID in the table.
[EnableNTPasOAM]	Defines the application type for NTP services. <ul style="list-style-type: none"> ▪ [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. <ul style="list-style-type: none"> ▪ [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.

A.1.3 Static Routing Parameters

The static routing parameters are described in the table below.

Table A-3: Static Routing Parameters

Parameter	Description
Static IP Routing Table	
Web/EMS: IP Routing Table [StaticRouteTable]	Defines up to 30 static IP routing rules for the device. These rules can be associated with IP interfaces defined in the Multiple Interface table (InterfaceTable parameter). The routing decision for sending the outgoing IP packet is based on the source subnet/VLAN. If not associated with an IP interface, the static IP rule is based on destination IP address. <p>When the destination of an outgoing IP packet does not match one of the subnets defined in the Multiple Interface table, the device searches this table for an entry that matches the requested destination host/network. If such an entry is found, the device sends the packet to the indicated router (i.e., next hop). If no explicit entry is found, the packet is sent to the default gateway according to the source interface of the packet (if defined).</p> The format of this parameter is as follows: [StaticRouteTable] FORMAT StaticRouteTable_Index = StaticRouteTable_InterfaceName, StaticRouteTable_Destination, StaticRouteTable_PrefixLength, StaticRouteTable_Gateway, StaticRouteTable_Description; [\StaticRouteTable] <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 102). ▪ The StaticRouteTable_Description parameter is a string value of up to 30 characters. ▪ The metric value (next hop) is automatically set to 1.

A.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 A-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. Note: For this parameter to take effect, a device reset is required.
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. Notes: <ul style="list-style-type: none"> ▪ The value for the Premium Control DiffServ is

Parameter	Description
	determined by the following (according to priority): <ul style="list-style-type: none"> ✓ 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: <ul style="list-style-type: none"> ▪ The value for the Premium Control DiffServ is determined by the following (according to priority): <ul style="list-style-type: none"> ✓ SigIPDiffserv value in the selected IP Profile (IPProfile parameter). ✓ PremiumServiceClassControlDiffServ.
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.
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.

A.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 A-5: NAT and STUN Parameters

Parameter	Description
STUN Parameters	
Web: Enable STUN EMS: STUN Enable [EnableSTUN]	Enables Simple Traversal of UDP through NATs (STUN). <ul style="list-style-type: none"> ▪ [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 more information on STUN, see STUN on page 126 . Notes: <ul style="list-style-type: none"> ▪ 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	Defines the IP address of the primary STUN server. The valid range is the legal IP addresses. The default value is

Parameter	Description
[STUNServerPrimaryIP]	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: <ul style="list-style-type: none"> 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.
NAT Parameters	
Web/EMS: NAT Traversal [DisableNAT]	Enables the NAT mechanism. <ul style="list-style-type: none"> [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]	Defines the 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. <ul style="list-style-type: none"> [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: <ul style="list-style-type: none"> The NAT mechanism must be enabled for this parameter to take

Parameter	Description
	effect (i.e., the parameter DisableNAT is set to 0). <ul style="list-style-type: none"> For information on RTP Multiplexing, see RTP Multiplexing (ThroughPacket) on page 157.
[EnableUDPPortTranslation]	Enables UDP port translation. <ul style="list-style-type: none"> [0] = Disables UDP port translation (default). [1] = Enables UDP port translation. 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: <ul style="list-style-type: none"> 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).

A.1.6 NFS Parameters

The Network File Systems (NFS) configuration parameters are described in the table below.

Table A-6: NFS Parameters

Parameter	Description
[NFSSBasePort]	Defines the start of the range of numbers used for local UDP ports used by the NFS client. The maximum number of local ports is maximum channels plus maximum NFS servers. The valid range is 0 to 65535. The default is 47000.
Web: NFS Table EMS: NFS Settings	
[NFSServers]	This <i>parameter</i> table 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: <ul style="list-style-type: none"> You can configure up to 16 NFS file systems (where the first index is

Parameter	Description
	<p>0).</p> <ul style="list-style-type: none"> ▪ 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 127. ▪ For a description of configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.1.7 DNS Parameters

The Domain name System (DNS) parameters are described in the table below.

Table A-7: DNS Parameters

Parameter	Description
Internal DNS Table	
Web: Internal DNS Table EMS: DNS Information [DNS2IP]	<p>This <i>parameter</i> table defines the internal DNS table for resolving host names into IP addresses. Up to four different IP addresses (in dotted-decimal notation) can be assigned to a host name. The format of this parameter is as follows:</p> <pre>[Dns2Ip] FORMAT Dns2Ip_Index = Dns2Ip_DomainName, Dns2Ip_FirstIpAddress, Dns2Ip_SecondIpAddress, Dns2Ip_ThirdIpAddress, Dns2Ip_FourthIpAddress; [\Dns2Ip]</pre> <p>For example: Dns2Ip 0 = DnsName, 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 <i>ini</i> file table parameter, see 'Configuring the Internal DNS Table' on page 123. ▪ For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Internal SRV Table	
Web: Internal SRV Table EMS: DNS Information [SRV2IP]	<p>This parameter table defines the internal SRV table for resolving host names into DNS A-Records. Three different A-Records can be assigned to a host name. Each A-Record contains the host name, priority, weight, and port. The format of this parameter is as follows:</p> <pre>[SRV2IP]</pre>

Parameter	Description
	<p>FORMAT SRV2IP_Index = SRV2IP_InternalDomain, SRV2IP_TransportType, SRV2IP_Dns1, SRV2IP_Priority1, SRV2IP_Weight1, SRV2IP_Port1, SRV2IP_Dns2, SRV2IP_Priority2, SRV2IP_Weight2, SRV2IP_Port2, SRV2IP_Dns3, SRV2IP_Priority3, SRV2IP_Weight3, SRV2IP_Port3; [\SRV2IP]</p> <p>For example: SRV2IP 0 = SrvDomain,0,Dnsname1,1,1,500,Dnsname2,2,2,501,\$\$,0,0,0;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 <i>ini</i> file table parameter, see 'Configuring the Internal SRV Table' on page 124. ▪ For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.1.8 DHCP Parameters

The Dynamic Host Control Protocol (DHCP) parameters are described in the table below.

Table A-8: DHCP Parameters

Parameter	Description
Web: Enable DHCP EMS: DHCP Enable [DHCPEnable]	<p>Enables Dynamic Host Control Protocol (DHCP) functionality.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable DHCP support on the device (default). ▪ [1] Enable = Enable DHCP support on the device. <p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ After you enable the DHCP server, perform the following procedure: <ol style="list-style-type: none"> 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 more information on DHCP, refer to the <i>Product Reference Manual</i>. ▪ This parameter is a special 'Hidden' parameter. Once defined and saved in flash memory, its assigned value doesn't revert to its default even if the parameter doesn't appear in the <i>ini</i> file.

Parameter	Description
EMS: DHCP Speed Factor [DHCPspeedFactor]	<p>Defines the DHCP renewal speed.</p> <ul style="list-style-type: none"> ▪ [0] = Disable ▪ [1] = Normal (default) ▪ [2] to [10] = Fast <p>When set to 0, the DHCP lease renewal is disabled. Otherwise, the renewal time is divided by this factor. Some DHCP-enabled routers perform better when set to 4.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>

A.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 A-9: NTP and Daylight Saving Time Parameters

Parameter	Description
NTP Parameters	
Note: For more information on Network Time Protocol (NTP), see 'Simple Network Time Protocol Support' on page 95.	
Web: NTP Server IP Address EMS: Server IP Address [NTPServerIP]	<p>Defines the IP address (in dotted-decimal notation) of the NTP server.</p> <p>The default IP address is 0.0.0.0 (i.e., internal NTP client is disabled).</p>
Web: NTP UTC Offset EMS: UTC Offset [NTPServerUTCOffset]	<p>Defines the Universal Time Coordinate (UTC) offset (in seconds) from the NTP server.</p> <p>The default offset is 0. The offset range is -43200 to 43200.</p>
Web: NTP Update Interval EMS: Update Interval [NTPUpdateInterval]	<p>Defines the time interval (in seconds) that the NTP client requests for a time update.</p> <p>The default interval is 86400 (i.e., 24 hours). The range is 0 to 214783647.</p> <p>Note: It is not recommend to set this parameter to beyond one month (i.e., 2592000 seconds).</p>
Daylight Saving Time Parameters	
Web: Day Light Saving Time EMS: Mode [DayLightSavingTimeEnable]	<p>Enables daylight saving time.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Web: Start Time EMS: Start [DayLightSavingTimeStart]	<p>Defines the date and time when daylight saving begins.</p> <p>The format of the value is mo:dd:hh:mm (month, day, hour, and minutes).</p>
Web: End Time EMS: End [DayLightSavingTimeEnd]	<p>Defines the date and time when daylight saving ends.</p> <p>The format of the value is mo:dd:hh:mm (month, day, hour, and minutes).</p>
Web/EMS: Offset [DayLightSavingTimeOffset]	<p>Defines the daylight saving time offset (in minutes).</p> <p>The valid range is 0 to 120. The default is 60.</p>

A.2 Management Parameters

This subsection describes the device's Web and Telnet parameters.

A.2.1 General Parameters

The general management parameters are described in the table below.

Table A-10: General Management 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.
Web: Use RADIUS for Web/Telnet Login EMS: Web Use Radius Login [WebRADIUSLogin]	Enables RADIUS queries for Web and Telnet authentication. <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable = Logging into the device's Web and Telnet embedded servers is done through a RADIUS server. The device contacts a user-defined server and verifies the given user name and password against a remote database, in a secure manner. Notes: <ul style="list-style-type: none"> ▪ 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).

A.2.2 Web Parameters

The Web parameters are described in the table below.

Table A-11: Web Parameters

Parameter	Description
Web: Deny Access On Fail Count [DenyAccessOnFailCount]	Defines the maximum number of login attempts after which the requesting IP address is blocked. The valid value range is 0 to 32768. The values 0 and 1 mean immediate block. The default is 3.

Parameter	Description
Web: Deny Authentication Timer [DenyAuthenticationTimer]	<p>Defines the time (in seconds) that login to the Web interface is denied for a user that has reached maximum login attempts as defined by the DenyAccessOnFailCount parameter. Only after this time expires can the user attempt to login from the same IP address.</p> <p>The default is 0.</p>
Web: Display Login Information [DisplayLoginInformation]	<p>Enables display of user's login information on each successful login attempt.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable
[EnableMgmtTwoFactorAuthentication]	<p>Enables Web login authentication using a third-party, smart card.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable <p>When enabled, the device retrieves the Web user's login username from the smart card, which is automatically displayed (read-only) in the Web Login screen; the user is then required to provide only the login password.</p> <p>Typically, a TLS connection is established between the smart card and the device's Web interface, and a RADIUS server is implemented to authenticate the password with the username. Thus, this feature implements a two-factor authentication - what the user has (the physical card) and what the user knows (i.e., the login password).</p>
[DisableWebTask]	<p>Enables device management through the Web interface.</p> <ul style="list-style-type: none"> ▪ [0] = Enable Web management (default). ▪ [1] = Disable Web management. <p>Note: For this parameter to take effect, a device reset is required.</p>
[HTTPport]	<p>Defines the LAN HTTP port for Web management (default is 80). To enable Web management from the LAN, configure the desired port.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: Disable WEB Config [DisableWebConfig]	<p>Determines whether the entire Web interface is read-only.</p> <ul style="list-style-type: none"> ▪ [0] = Enables modifications of parameters (default). ▪ [1] = Web interface is read-only. <p>When in read-only mode, parameters can't be modified. In addition, the following pages can't be accessed: 'Web User Accounts', 'Certificates', 'Regional Settings', 'Maintenance Actions' and all file-loading pages ('Load Auxiliary Files', 'Software Upgrade Wizard', and 'Configuration File').</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Determines whether the device resets the username and password of the primary and secondary accounts to their default settings.</p> <ul style="list-style-type: none"> [0] = Password and username retain their values (default). [1] = Password and username are reset. <p>Notes:</p> <ul style="list-style-type: none"> 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 <i>ini</i> file).
[ScenarioFileName]	<p>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 54.</p>
[WelcomeMessage]	<p>This <i>parameter</i> table defines the Welcome message that appears after a Web interface login. The format of this parameter is as follows:</p> <pre>[WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text [WelcomeMessage]</pre> <p>For Example:</p> <pre>FORMAT WelcomeMessage_Index = WelcomeMessage_Text WelcomeMessage 1 = "*****" ; WelcomeMessage 2 = "***** This is a Welcome message ***" ; WelcomeMessage 3 = "*****" ;</pre> <p>Notes:</p> <ul style="list-style-type: none"> 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 <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.2.3 Telnet Parameters

The Telnet parameters are described in the table below.

Table A-12: Telnet Parameters

Parameter	Description
Web: Embedded Telnet Server EMS: Server Enable [TelnetServerEnable]	<p>Enables the device's embedded Telnet server. Telnet is disabled by default for security.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable Unsecured [2] Enable Secured (SSL) <p>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).</p>

Parameter	Description
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.

A.2.4 SNMP Parameters

The SNMP parameters are described in the table below.

Table A-13: SNMP Parameters

Parameter	Description
Web: Enable SNMP [DisableSNMP]	Enables SNMP. <ul style="list-style-type: none"> [0] Enable = SNMP is enabled (default). [1] Disable = SNMP is disabled and no traps are sent.
[SNMPPort]	Defines the device's local (LAN) UDP port used for SNMP Get/Set commands. The range is 100 to 3999. The default port is 161. Note: For 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: <ul style="list-style-type: none"> 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.
[ChassisPhysicalAlias]	Defines the 'alias' name object for the physical entity as specified by a network manager, and provides a non-volatile 'handle' for the physical entity. The valid range is a string of up to 255 characters.
[ChassisPhysicalAssetID]	Defines the user-assigned asset tracking identifier object for the device's chassis as specified by an EMS, and provides non-volatile storage of this information. The valid range is a string of up to 255 characters.
[ifAlias]	Defines the textual name of the interface. The value is equal to the ifAlias SNMP MIB object. The valid range is a string of up to 64 characters.
EMS: Keep Alive Trap Port [KeepAliveTrapPort]	Defines the port to which keep-alive traps are sent. The valid range is 0 - 65534. The default is port 162.

Parameter	Description
[SendKeepAliveTrap]	<p>Enables keep-alive traps and sends them every 9/10 of the time as defined by the NATBindingDefaultTimeout parameter.</p> <ul style="list-style-type: none"> [0] = Disable [1] = Enable <p>Note: For this parameter to take effect, a device reset is required.</p>
[SNMPSysOid]	<p>Defines the base product system OID. The default is eSNMP_AC_PRODUCT_BASE_OID_D.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[SNMPTrapEnterpriseOid]	<p>Defines the Trap Enterprise OID. The default is eSNMP_AC_ENTERPRISE_OID. The inner shift of the trap in the AcTrap subtree is added to the end of the OID in this parameter.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[acUserInputAlarmDescription]	Defines the description of the input alarm.
[acUserInputAlarmSeverity]	Defines the severity of the input alarm.
[AlarmHistoryTableMaxSize]	<p>Defines the maximum number of rows in the Alarm History table. This parameter can be controlled by the Config Global Entry Limit MIB (located in the Notification Log MIB). The valid range is 50 to 1000. The default value is 500.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[SNMPEngineIDString]	<p>Defines the SNMP engine ID for SNMPv2/SNMPv3 agents. This is used for authenticating a user attempting to access the SNMP agent on the device.</p> <p>The ID can be a string of up to 36 characters. The default value is 00:00:00:00:00:00:00:00:00:00:00:00:00 (12 Hex octets characters). The provided key must be set with 12 Hex values delimited by a colon (":") in the format xx:xx:....xx. For example, 00:11:22:33:44:55:66:77:88:99:aa:bb</p> <p>Notes:</p> <ul style="list-style-type: none"> 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.
<p>Web: SNMP Trap Destination Parameters EMS: Network > SNMP Managers Table Note: Up to five SNMP trap managers can be defined.</p>	
SNMP Manager [SNMPManagerIsUsed_x]	<p>Determines the validity of the parameters (IP address and port number) of the corresponding SNMP Manager used to receive SNMP traps.</p> <ul style="list-style-type: none"> [0] (Check box cleared) = Disabled (default) [1] (Check box selected) = Enabled
Web: IP Address EMS: Address [SNMPManagerTableIP_x]	<p>Defines the IP address of the remote host used as an SNMP Manager. The device sends SNMP traps to this IP address. Enter the IP address in dotted-decimal notation, e.g., 108.10.1.255.</p>

Parameter	Description
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]	Enables the sending of traps to the corresponding SNMP manager. <ul style="list-style-type: none"> [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: 'mngnr.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]	Defines the Community string used in traps (up to 19 characters). The default string is 'trapuser'.
Web: SNMP V3 Table EMS: SNMP V3 Users	
[SNMPUsers]	This <i>parameter</i> table defines 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: <ul style="list-style-type: none"> 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 78. For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84

A.2.5 Serial Parameters

The RS-232 serial parameters are described in the table below.

Table A-14: Serial Parameters

Parameter	Description
[DisableRS232]	<p>Enables the device's RS-232 (serial) port.</p> <ul style="list-style-type: none"> ▪ [0] = Enabled (default) ▪ [1] = Disabled <p>The RS-232 serial port can be used to change the networking parameters and view error/notification messages. For how to establish a serial communication with the device, refer to the <i>Installation Manual</i>.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: Baud Rate [SerialBaudRate]	<p>Defines the RS-232 baud rate.</p> <p>The valid values include the following: 1200, 2400, 9600, 14400, 19200, 38400, 57600, or 115200 (default).</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: Data [SerialData]	<p>Defines the RS-232 data bit.</p> <ul style="list-style-type: none"> ▪ [7] = 7-bit. ▪ [8] = 8-bit (default). <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: Parity [SerialParity]	<p>Defines the RS-232 polarity.</p> <ul style="list-style-type: none"> ▪ [0] = None (default). ▪ [1] = Odd. ▪ [2] = Even. <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: Stop [SerialStop]	<p>Defines the RS-232 stop bit.</p> <ul style="list-style-type: none"> ▪ [1] = 1-bit (default). ▪ [2] = 2-bit. <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: Flow Control [SerialFlowControl]	<p>Defines the RS-232 flow control.</p> <ul style="list-style-type: none"> ▪ [0] = None (default). ▪ [1] = Hardware. <p>Note: For this parameter to take effect, a device reset is required.</p>

A.3 Debugging and Diagnostics Parameters

This subsection describes the device's debugging and diagnostic parameters.

A.3.1 General Parameters

The general debugging and diagnostic parameters are described in the table below.

Table A-15: General Debugging and Diagnostic Parameters

Parameter	Description
EMS: Enable Diagnostics [EnableDiagnostics]	<p>Determines the method for verifying correct functioning of the different hardware components on the device. On completion of the check and if the test fails, the device sends information on the test results of each hardware component to the Syslog server.</p> <ul style="list-style-type: none"> ▪ [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). <p>For more information, refer to the <i>Product Reference Manual</i>.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: Enable LAN Watchdog [EnableLanWatchDog]	<p>Enables the LAN watchdog feature.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable. <p>When LAN watchdog is enabled, the device's overall communication integrity is checked periodically. If no communication is detected for about three minutes, the device performs a self test:</p> <ul style="list-style-type: none"> ▪ 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). ▪ If the self-test fails, the device restarts to overcome internal fatal communication error. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ Enable LAN watchdog is relevant only if the Ethernet connection is full duplex.
[WatchDogStatus]	<p>Enables the device's watchdog feature.</p> <ul style="list-style-type: none"> ▪ [0] = Disable. ▪ [1] = Enable (default). <p>Note: For this parameter to take effect, a device reset is required.</p>
[LifeLineType]	<p>Defines the scenario upon which the Lifeline analog (FXS) feature is activated. The Lifeline feature can be activated upon a power outage, physical disconnection of the LAN cable, or network failure (i.e., loss of IP connectivity). Upon any of these scenarios, the Lifeline feature provides PSTN connectivity (and call continuity) for the FXS phone users.</p> <p>The Lifeline (FXS) phone is connected to the following port:</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ FXS Port 1 of each FXS module FXS Port 1 connects to the POTS (Lifeline) phone as well as to the PSTN / PBX, using a splitter cable. <ul style="list-style-type: none"> ▪ [0] = Lifeline is activated upon power outage (default). ▪ [1] = Lifeline is activated upon power outage or when the link is down (physically disconnected). ▪ [2] = Lifeline is activated upon a power outage, when the link is down (physically disconnected), or upon network failure (logical link disconnected). Notes: <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is applicable only to FXS interfaces. ▪ To enable Lifeline upon a network failure, the LAN watch dog must be activated (i.e., set the parameter EnableLANWatchDog to 1). ▪ A Lifeline phone connection can be setup for each FXS module (using Port 1) housed in the chassis. ▪ For information on Lifeline cabling, 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.
[Mediant1000DualPowerSupplySupported]	Determines whether the device sends raised alarms (to the SNMP client and/or Web interface) concerned with the Power Supply modules. <ul style="list-style-type: none"> ▪ [1] (default) = No alarms are sent. ▪ [2] = The device sends alarms if one of the Power Supply modules is removed from the chassis. These alarms are reflected in the SNMP and Web interface. Notes: <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ If this parameter is set to 2 and for this feature to be functional, both Main and Redundant Power Supply modules must be present in the chassis.
[GroundKeyDetection]	Enables analog ground-key detection for the device. The device's FXS and FXO modules implement ground-start signaling. When disabled, the device uses loop-start signaling. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable (enables ground start) Notes: <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ For ground-start signaling, ensure that the FXO G module is installed (and not the regular FXO module) in the device's chassis. ▪ For FXO ground-start signaling, ensure that the parameter EnableCurrentDisconnect is set to 1 and the parameter FXOBetweenRingTime is set to 300. ▪ FXS ground-start interface does not generate a ringing voltage.

Parameter	Description
	The FXS interface initiates the signaling by grounding of the TIP lead.

A.3.2 Syslog, CDR and Debug Parameters

The Syslog, CDR and debug parameters are described in the table below.

Table A-16: Syslog, CDR and Debug Parameters

Parameter	Description
Web: Enable Syslog EMS: Syslog enable [EnableSyslog]	Determines whether the device sends logs and error messages generated by the device to a Syslog server. <ul style="list-style-type: none"> ▪ [0] Disable = Logs and errors are not sent to the Syslog server (default). ▪ [1] Enable = Enables the Syslog server. Notes: <ul style="list-style-type: none"> ▪ If you enable Syslog, you must enter an IP address of the Syslog server (using the SyslogServerIP parameter). ▪ Syslog messages may increase the network traffic. ▪ To configure Syslog SIP message logging levels, use the GwDebugLevel parameter. ▪ For more information on Syslog, refer to the <i>Product Reference Manual</i>. ▪ By default, logs are also sent to the RS-232 serial port. For how to establish serial communication with the device, refer to the Installation Manual.
Web/EMS: Syslog Server IP Address [SyslogServerIP]	Defines the IP address (in dotted-decimal notation) of the computer on which the Syslog server is running. The Syslog server is an application designed to collect the logs and error messages generated by the device. Default IP address is 0.0.0.0. For information on Syslog, refer to the <i>Product Reference Manual</i> .
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 Syslog, refer to the <i>Product Reference Manual</i> .
[MaxBundleSyslogLength]	Defines the maximum size (in bytes) threshold of logged Syslog messages bundled into a single UDP packet, after which they are sent to a Syslog server. The valid value range is 0 to 1220 (where 0 indicates that no bundling occurs). The default is 1220. Note: 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: <ul style="list-style-type: none"> ▪ The CDR messages are sent to UDP port 514 (default Syslog port). ▪ This mechanism is active only when Syslog is enabled (i.e., the

Parameter	Description
Web/EMS: CDR Report Level [CDRReportLevel]	<p>parameter EnableSyslog is set to 1).</p> <p>Determines whether Call Detail Records (CDR) are sent to the Syslog server and when they are sent.</p> <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Defines the Syslog debug logging level.</p> <ul style="list-style-type: none"> ▪ [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: <ul style="list-style-type: none"> ✓ 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. <p>Note that when this option is used, in order to read Syslog messages with Wireshark, a special plug-in (i.e., acsyslog.dll) must be used. Once the plug-in is installed, the Syslog messages are decoded as "AC SYSLOG" and are displayed using the 'acsyslog' filter instead of the regular 'syslog' filter.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Defines the Facility level (0 through 7) of the device's Syslog messages, according to RFC 3164. This allows you to identify Syslog messages generated by the device. This is useful, for example, if you collect the device's and other equipments' Syslog messages, at one single server. The device's Syslog messages can easily be identified and distinguished from other Syslog messages by its Facility level. Therefore, in addition to filtering Syslog messages according to IP address, the messages can be filtered according to Facility level.</p> <ul style="list-style-type: none"> ▪ [16] = local use 0 (local0) - default ▪ [17] = local use 1 (local1)

Parameter	Description
	<ul style="list-style-type: none"> ▪ [18] = local use 2 (local2) ▪ [19] = local use 3 (local3) ▪ [20] = local use 4 (local4) ▪ [21] = local use 5 (local5) ▪ [22] = local use 6 (local6) ▪ [23] = local use 7 (local7)
<p>Web: Activity Types to Report via Activity Log Messages</p> <p>[ActivityListToLog]</p>	<p>Defines the Activity Log mechanism of the device, which sends log messages (to a Syslog server) for reporting certain types of Web operations according to the below user-defined filters.</p> <ul style="list-style-type: none"> ▪ [pvc] Parameters Value Change = Changes made on-the-fly to parameters. ▪ [aff] 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: <ul style="list-style-type: none"> ✓ (1) ini parameters (AdminPage) ✓ (2) General Security Settings ✓ (3) Configuration File ✓ (4) IP Security Proposal / IP Security Associations Tables ✓ (5) Software Upgrade Key Status ✓ (6) Firewall Settings ✓ (7) Web & Telnet 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: <ul style="list-style-type: none"> ✓ (1) IP Address ✓ (2) Subnet Mask ✓ (3) Default Gateway IP Address ✓ (4) ActivityListToLog ▪ [ll] Login and Logout = Every login and logout attempt. <p>For example: ActivityListToLog = 'pvc', 'aff', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc'</p> <p>Note: For the <i>ini</i> file, values must be enclosed in single quotation marks.</p>
<p>[FacilityTrace]</p>	<p>Enables ISDN traces of Facility Information Elements (IE) for ISDN call diagnostics. This allows you to trace all the parameters contained in the Facility IE and view them in the Syslog.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note: For this feature to be functional, the GWDebugLevel parameter must be enabled (i.e., set to at least level 1).</p>

A.3.3 Resource Allocation Indication Parameters

The Resource Allocation Indication (RAI) parameters are described in the table below.

Table A-17: RAI Parameters

Parameter	Description
[EnableRAI]	Enables RAI alarm generation if the device's busy endpoints exceed a user-defined threshold. <ul style="list-style-type: none"> ▪ [0] = Disable RAI (Resource Available Indication) service (default). ▪ [1] = RAI service enabled and an SNMP 'acBoardCallResourcesAlarm' Alarm Trap is sent.
[RAIHighThreshold]	Defines the high threshold percentage of total calls that are active (busy endpoints). When the percentage of the device's busy endpoints exceeds this high threshold, the device sends the SNMP acBoardCallResourcesAlarm alarm trap with a 'major' alarm status. The range is 0 to 100. The default value is 90. <p>Note: The percentage of busy endpoints is calculated by dividing the number of busy endpoints by the total number of "enabled" endpoints (trunks are physically connected and synchronized with no alarms and endpoints are defined in the Trunk Group Table).</p>
[RAILowThreshold]	Defines the low threshold percentage of total calls that are active (busy endpoints). When the percentage of the device's busy endpoints falls below this low threshold, the device sends an SNMP acBoardCallResourcesAlarm alarm trap with a 'cleared' alarm status. The range is 0 to 100%. The default value is 90%.
[RAILoopTime]	Defines the time interval (in seconds) that the device periodically checks call resource availability. The valid range is 1 to 200. The default is 10.
[EnableAutoRAITransmitBER]	Enables the device to send RAI when the bit error rate (BER) is above 0.001. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable

A.3.4 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 A-18: BootP Parameters

Parameter	Description	
[BootPRetries]	<p>Note: For this parameter to take effect, a device reset is required. This parameter is used to:</p>	
	Defines the number of BootP requests that the device sends during start-up. The device stops sending BootP requests when either BootP reply is received or	Defines the number of DHCP packets that the device sends. If after all packets are sent there's still no reply, the device loads from

Parameter	Description	
	number of retries is reached. <ul style="list-style-type: none"> ▪ [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. 	flash. <ul style="list-style-type: none"> ▪ [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
[BootPSelectiveEnable]	Enables the Selective BootP mechanism. <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	Defines the interval between the device's startup and the first BootP/DHCP request that is issued by the device. <ul style="list-style-type: none"> ▪ [1] = 1 second (default). ▪ [2] = 3 second. ▪ [3] = 6 second. ▪ [4] = 30 second. ▪ [5] = 60 second. <p>Note: For this parameter to take effect, a device reset is required.</p>	
[ExtBootPReqEnable]	Determines whether the device uses the Vendor Specific Information field in the BootP request to provide device-related initial startup information. <ul style="list-style-type: none"> ▪ [0] = Disabled (default). ▪ [1] = Enables extended information to be sent in BootP requests. 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 <i>Product Reference Manual</i>. The BootP/TFTP configuration utility displays this information in the 'Client Info' column. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ This option is not available on DHCP servers. 	

A.4 Security Parameters

This subsection describes the device's security parameters.

A.4.1 General Parameters

The general security parameters are described in the table below.

Table A-19: General Security Parameters

Parameter	Description
Web: Voice Menu Password [VoiceMenuPassword]	Defines the password for accessing the device's voice menu, used for configuring and monitoring the device. To activate the menu, connect a POTS telephone (i.e., to the FXS port) and dial *** (three stars) followed by the password. The default value is 12345. Notes: <ul style="list-style-type: none"> ▪ To disable the Voice Menu, do any of the following: <ul style="list-style-type: none"> ✓ Set the VoiceMenuPassword parameter to 'disable'. ✓ Change the Web login password for the Admin user from its default value (i.e., 'Admin') to any other value, and then reset the device. ▪ This parameter is applicable only to FXS interfaces. ▪ For more information on the Voice menu, refer to the Installation Manual.
[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. <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable = disables TFTP and allows secure protocols such as HTTPS to fetch the device configuration. For more information 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 <i>parameter</i> table defines 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_Source_Port, AccessList_PrefixLen, AccessList_Source_Port, AccessList_Start_Port, AccessList_End_Port, AccessList_Protocol, AccessList_Use_Specific_Interface, AccessList_Interface_ID, AccessList_Packet_Size, AccessList_Byte_Rate, AccessList_Byte_Burst, AccessList_Allow_Type; [AccessList] For example:

Parameter	Description
	<p>AccessList 10 = mgmt.customer.com, , , 32, 0, 80, tcp, 1, OAMP, 0, 0, 0, allow;</p> <p>AccessList 22 = 10.4.0.0, , , 16, 4000, 9000, any, 0, , 0, 0, 0, block;</p> <p>In the example above, Rule #10 allows traffic from the host 'mgmt.customer.com' destined to TCP ports 0 to 80 on interface OAMP (OAMP). Rule #22 blocks traffic from the subnet 10.4.xxx.yyy destined to ports 4000 to 9000.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 <i>ini</i> file table parameter, see 'Configuring Firewall Settings' on page 131. ▪ For a description of configuring with <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.4.2 HTTPS Parameters

The Secure Hypertext Transport Protocol (HTTPS) parameters are described in the table below.

Table A-20: HTTPS Parameters

Parameter	Description
Web: Secured Web Connection (HTTPS) EMS: HTTPS Only [HTTPSOnly]	<p>Determines the protocol used to access the Web interface.</p> <ul style="list-style-type: none"> ▪ [0] HTTP and HTTPS (default). ▪ [1] HTTPs Only = Unencrypted HTTP packets are blocked. <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: HTTPS Port [HTTPSPort]	<p>Defines the local Secured HTTPS port of the device. This parameter allows secure remote device Web management from the LAN. To enable secure Web management from the LAN, configure the desired port.</p> <p>The valid range is 1 to 65535 (other restrictions may apply within this range). The default port is 443.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: HTTPS Cipher String [HTTSPCipherString]	<p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ If the "Strong Encryption" Software Upgrade Key is enabled, the default of the HTTSPCipherString parameter is changed to 'RC4:EXP', enabling RC-128bit encryption. ▪ The value 'ALL' can be configured only if the "Strong Encryption" Software Upgrade Key is enabled.

Parameter	Description
Web: HTTP Authentication Mode EMS: Web Authentication Mode [WebAuthMode]	Determines the authentication mode used for the Web interface. <ul style="list-style-type: none"> ▪ [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. <p>Note: When RADIUS login is enabled (i.e., the parameter WebRADIUSLogin is set to 1), basic authentication is forced.</p>
[HTTPSRequireClientCertificate]	Determines whether client certificates are required for HTTPS connection. <ul style="list-style-type: none"> ▪ [0] = Client certificates are not required (default). ▪ [1] = Client certificates are required. The client certificate must be preloaded to the device and its matching private key must be installed on the managing PC. Time and date must be correctly set on the device for the client certificate to be verified. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ For a description on implementing client certificates, see 'Client Certificates' on page 93.
[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. <p>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.</p>
[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. <p>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.</p>

A.4.3 SRTP Parameters

The Secure Real-Time Transport Protocol (SRTP) parameters are described in the table below.

Table A-21: SRTP Parameters

Parameter	Description
Web: Media Security EMS: Enable Media Security [EnableMediaSecurity]	<p>Enables Secure Real-Time Transport Protocol (SRTP).</p> <ul style="list-style-type: none"> ▪ [0] Disable = SRTP is disabled (default). ▪ [1] Enable = SRTP is enabled. <p>Note: For this parameter to take effect, a device reset is required.</p>
Web/EMS: Media Security Behavior [MediaSecurityBehaviour]	<p>Determines the device's mode of operation when SRTP is used (i.e., when the parameter EnableMediaSecurity is set to 1).</p> <ul style="list-style-type: none"> ▪ [0] Preferable = The device initiates encrypted calls. However, if negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted. (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 IP Profile for which this parameter is set 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. The remote UA can respond with SRTP or RTP parameters: <ul style="list-style-type: none"> ✓ If the remote SIP UA does not support SRTP, it uses RTP and ignores the crypto lines. ✓ In the opposite direction, if the device receives an SDP offer with a single media (as shown above), it responds with SRTP (RTP/SAVP) if the EnableMediaSecurity parameter is set to 1. If SRTP is not supported (i.e., EnableMediaSecurity is set to 0), it responds with RTP. <p>Notes:</p> <ul style="list-style-type: none"> ▪ Before configuring this parameter, set the EnableMediaSecurity parameter to 1. ▪ Option [2] Disable is applicable only to IP Profiles. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 217).
Web: Master Key Identifier (MKI) Size EMS: Packet MKI Size [SRTPTxPacketMKISize]	<p>Defines 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.</p>
[EnableSymmetricMKI]	<p>Enables symmetric MKI negotiation.</p> <ul style="list-style-type: none"> ▪ [0] = Disabled (default) - the device includes the MKI in its 200 OK response according to the SRTPTxPacketMKISize parameter (if set to 0, then it is not included; if set to any other value, it is included with this value). ▪ [1] = Enabled - the answer crypto line contains (or excludes) an MKI value according to the selected crypto line in the offer. For example, assume that the device receives an INVITE containing

Parameter	Description
	<p>the following two crypto lines in SDP:</p> <pre>a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:TAaxNnQt8/qLQMnDuG4vxYfWl6K7eBK/ufk04pR4 2^ 31 1:1 a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:bnuYZnMxSfUiGitviWJZmzr7OF3AiRO015Vnh0kH 2^ 31</pre> <p>The first crypto line includes the MKI parameter "1:1". In the 200 OK response, the device selects one of the crypto lines (i.e., '2' or '3'). If it selects crypto line '2', it includes the MKI parameter in its answer SDP, for example:</p> <pre>a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:RlVyAlxV/qwBjkEkl4kSJy13wCtYeZLq1/QFuxw 2^ 31 1:1</pre> <p>If the device selects a crypto line that does not contain the MKI parameter, then the MKI parameter is not included in the crypto line in the SDP answer (even if the SRTPTxPacketMKISize parameter is set to any value other than 0).</p> <p>Note: To enable symmetric MKI, the SRTPTxPacketMKISize parameter must be set to any value other than 0.</p>
Web/EMS: SRTP offered Suites [SRTPofferedSuites]	Defines the offered crypto suites (cipher encryption algorithms) for SRTP. <ul style="list-style-type: none"> ▪ [0] = All available crypto suites (default) ▪ [1] CIPHER SUITES AES CM 128 HMAC SHA1 80 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 80-bit tag. ▪ [2] CIPHER SUITES AES CM 128 HMAC SHA1 32 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag.
Web: Disable Authentication On Transmitted RTP Packets EMS: RTP AuthenticationDisable Tx [RTPAuthenticationDisableTx]	Enables authentication on transmitted RTP packets in a secured RTP session. <ul style="list-style-type: none"> ▪ [0] Enable (default) ▪ [1] Disable
Web: Disable Encryption On Transmitted RTP Packets EMS: RTP EncryptionDisable Tx [RTPEncryptionDisableTx]	Enables encryption on transmitted RTP packets in a secured RTP session. <ul style="list-style-type: none"> ▪ [0] Enable (default) ▪ [1] Disable
Web: Disable Encryption On Transmitted RTCP Packets EMS: RTCP EncryptionDisable Tx [RTCPEncryptionDisableTx]	Enables encryption on transmitted RTCP packets in a secured RTP session. <ul style="list-style-type: none"> ▪ [0] Enable (default) ▪ [1] Disable

A.4.4 TLS Parameters

The Transport Layer Security (TLS) parameters are described in the table below.

Table A-22: TLS Parameters

Parameter	Description
Web/EMS: TLS Version [TLSVersion]	<p>Determines the supported versions of SSL/TLS (Secure Socket Layer/Transport Layer Security).</p> <ul style="list-style-type: none"> ▪ [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. <p>When set to 0, SSL/TLS handshakes always start with SSL 2.0 and switch to TLS 1.0 if both peers support it. When set to 1, TLS 1.0 is the only version supported; clients attempting to contact the device using SSL 2.0 are rejected.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: TLS Client Re-Handshake Interval EMS: TLS Re Handshake Interval [TLSReHandshakeInterval]	<p>Defines the time interval (in minutes) between TLS Re-Handshakes initiated by the device.</p> <p>The interval range is 0 to 1,500 minutes. The default is 0 (i.e., no TLS Re-Handshake).</p>
Web: TLS Mutual Authentication EMS: SIPS Require Client Certificate [SIPSRequireClientCertificate]	<p>Determines the device's behavior when acting as a server for TLS connections.</p> <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ The SIPS certificate files can be changed using the parameters HTTPSCertFileName and HTTPSPRootFileName.
Web/EMS: Peer Host Name Verification Mode [PeerHostNameVerificationMode]	<p>Determines whether the device verifies the Subject Name of a remote certificate when establishing TLS connections.</p> <ul style="list-style-type: none"> ▪ [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. <p>When a remote certificate is received and this parameter is not disabled, the value of SubjectAltName is compared with the list of available Proxies. If a match is found for any of the configured Proxies, the TLS connection is established.</p> <p>The comparison is performed if the SubjectAltName is either a DNS name (DNSName) or an IP address. If no match is found and the SubjectAltName is marked as 'critical', the TLS connection is not established. If DNSName is used, the certificate can also use wildcards ("*") to replace parts of the domain name.</p> <p>If the SubjectAltName is not marked as 'critical' and there is no</p>

Parameter	Description
	match, the CN value of the SubjectName field is compared with the parameter TLSRemoteSubjectName. If a match is found, the connection is established. Otherwise, the connection is terminated.
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. <ul style="list-style-type: none"> ▪ [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.
Web: Client Cipher String [TLSClientCipherString]	Defines the cipher-suite string for TLS clients. The valid value is up to 255 strings. The default is "ALL:!ADH". For example: TLSClientCipherString = 'EXP' This parameter complements the HTTPSCipherString parameter (which affects TLS servers). For possible values and additional details, refer to: http://www.openssl.org/docs/apps/ciphers.html
[TLSPkeySize]	Defines the key size (in bits) for RSA public-key encryption for newly self-signed generated keys for SSH. <ul style="list-style-type: none"> ▪ [512] ▪ [768] ▪ [1024] (default) ▪ [2048]

A.4.5 SSH Parameters

Secure Shell (SSH) parameters are described in the table below.

Table A-23: SSH Parameters

Parameter	Description
Web/EMS: Enable SSH Server [SSHServerEnable]	Enables the device's embedded SSH server. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable
Web/EMS: Server Port [SSHServerPort]	Defines the port number for the embedded SSH server. Range is any valid port number. The default port is 22.
Web: SSH Admin Key [SSHAdminKey]	Defines the RSA public key for strong authentication for logging in to the SSH interface (if enabled). The value should be a base64-encoded string. The value can be a maximum length of 511 characters. For more information, refer to the <i>Product Reference Manual</i> .
Web: Require Public Key [SSHRequirePublicKey]	Enables RSA public keys for SSH. <ul style="list-style-type: none"> [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.
Web: Max Payload Size [SSHMaxPayloadSize]	Defines the maximum uncompressed payload size (in bytes) for SSH packets. The valid value is 550 to 32768. The default is 32768.
Web: Max Binary Packet Size [SSHMaxBinaryPacketSize]	Defines the maximum packet size (in bytes) for SSH packets. The valid value is 582 to 35000. The default is 35000.
[SSHMaxSessions]	Defines the maximum number of simultaneous SSH sessions. The valid range is 1 to 2. The default is 2 sessions.
Web: Enable Last Login Message [SSHEnableLastLoginMessage]	Enables message display in SSH sessions of the time and date of the last SSH login. The SSH login message displays the number of unsuccessful login attempts since the last successful login. <ul style="list-style-type: none"> [0] Disable [1] Enable (default) Note: The last SSH login information is cleared when the device is reset.
Web: Max Login Attempts [SSHMaxLoginAttempts]	Defines the maximum SSH login attempts allowed for entering an incorrect password by an administrator before the SSH session is rejected. The valid range is 1 to 3. the default is 3.

A.4.6 IPsec Parameters

The Internet Protocol security (IPsec) parameters are described in the table below.

Table A-24: IPsec Parameters

Parameter	Description
IPsec Parameters	
Web: Enable IP Security EMS: IPsec Enable [EnableIPsec]	Enables IPsec on the device. <ul style="list-style-type: none"> ▪ [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]	<p>This <i>parameter</i> table defines 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:</p> <pre>[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]</pre> <p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 137. ▪ For configuring ini file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Web: IP Security Proposal Table EMS: IPsec Proposal Table	
[IPsecProposalTable]	<p>This <i>parameter</i> table defines up to four IKE proposal settings, where each proposal defines an encryption algorithm, an authentication algorithm, and a Diffie-Hellman group identifier.</p>

Parameter	Description
	<p>[IPsecProposalTable] FORMAT IPsecProposalTable_Index = IPsecProposalTable_EncryptionAlgorithm, IPsecProposalTable_AuthenticationAlgorithm, IPsecProposalTable_DHGroup; [\IPsecProposalTable]</p> <p>For example: IPsecProposalTable 0 = 3, 2, 1; IPsecProposalTable 1 = 2, 2, 1;</p> <p>In the example above, two proposals are defined:</p> <ul style="list-style-type: none"> ▪ Proposal 0: AES, SHA1, DH group 2 ▪ Proposal 1: 3DES, SHA1, DH group 2 <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 135. ▪ For configuring ini file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.4.7 OCSP Parameters

The Online Certificate Status Protocol (OCSP) parameters are described in the table below.

Table A-25: OCSP Parameters

Parameter	Description
Web: Enable OCSP Server EMS: OCSP Enable [OCSPEnable]	Enables or disables certificate checking using OCSP. <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable. For a description of OCSP, refer to the <i>Product Reference Manual</i> .
Web: Primary Server IP EMS: OCSP Server IP [OCSPServerIP]	Defines the IP address of the OCSP server. The default IP address is 0.0.0.0.
Web: Secondary Server IP [OCSPSecondaryServerIP]	Defines the IP address (in dotted-decimal notation) of the secondary OCSP server (optional). The default IP address is 0.0.0.0.
Web: Server Port EMS: OCSP Server Port [OCSPServerPort]	Defines the OCSP server's TCP port number. The default port number is 2560.
Web: Default Response When Server Unreachable EMS: OCSP Default Response [OCSPDefaultResponse]	Determines the default OCSP behavior when the server cannot be contacted. <ul style="list-style-type: none"> ▪ [0] Disable = Rejects peer certificate (default). ▪ [1] Enable = Allows peer certificate.

A.5 RADIUS Parameters

The RADIUS parameters are described in the table below. For supported RADIUS attributes, see 'Supported RADIUS Attributes' on page 517.

Table A-26: RADIUS Parameters

Parameter	Description
Web: Enable RADIUS Access Control [EnableRADIUS]	Enables the RADIUS application. <ul style="list-style-type: none"> ▪ [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]	Defines the IP address of the RADIUS accounting server.
Web: Accounting Port [RADIUSAccPort]	Defines the 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. <ul style="list-style-type: none"> ▪ [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.
Web: AAA Indications EMS: Indications [AAAIndications]	Determines the Authentication, Authorization and Accounting (AAA) indications. <ul style="list-style-type: none"> ▪ [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. <ul style="list-style-type: none"> ▪ [0] Deny Access = Denies access. ▪ [1] Verify Access Locally = Checks password locally (default).
[MaxRADIUSSessions]	Defines the 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]	Defines the number of retransmission retries. The valid range is 1 to 10. The default value is 3.
[RadiusTO]	Defines the time interval (measured in seconds) that the device waits for a response before a RADIUS retransmission is issued. The valid range is 1 to 30. The default value is 10.
Web: RADIUS Authentication Server IP Address [RADIUSAuthServerIP]	Defines the 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]	Defines the port of the RADIUS Authentication Server. Note: For this parameter to take effect, a device reset is required.
Web: RADIUS Shared Secret [SharedSecret]	Defines the 'Secret' used to authenticate the device to the RADIUS server. This should be a cryptically strong password.
Web: Default Access Level	Defines the default access level for the device when the RADIUS

Parameter	Description
[DefaultAccessLevel]	(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]	Determines the device's mode of operation regarding the timer (configured by the parameter RadiusLocalCacheTimeout) that determines the validity of the user name and password (verified by the RADIUS server). <ul style="list-style-type: none"> ▪ [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 0xFFFFFFFF. The default value is 300 (5 minutes). <ul style="list-style-type: none"> ▪ [-1] = Never expires. ▪ [0] = Each request requires RADIUS authentication.
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.

A.6 SIP Media Realm Parameters

The Media Realm parameters are described in the table below.

Table A-27: Media Realm Parameters

Parameter	Description
Media Realm Table	
Web: Media Realm Table EMS: Protocol Definition > Media Realm [CpMediaRealm]	This <i>parameter</i> table defines the Media Realm table. The Media Realm table allows you to divide a Media-type interface (defined in the Multiple Interface table) into several realms, where each realm is specified by a UDP port range. 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_TransRateRatio, CpMediaRealm_IsDefault;

Parameter	Description
	<p>[\CpMediaRealm]</p> <p>For example, CpMediaRealm 1 = Mrealm1, Voice, , 6600, 20, 6790, , 1; CpMediaRealm 2 = Mrealm2, Voice, , 6800, 10, 6890; , 0;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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. ▪ 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. ▪ For a detailed description of all the parameters included in this <i>ini</i> file table parameter and for configuring Media Realms using the Web interface, see 'Configuring Media Realms' on page 170. ▪ For a description on configuring ini file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.7 Quality of Experience Reporting

The Quality of Experience parameters are described in the table below.

Table A-28: Quality of Experience Parameters

Parameter	Description
[QOEServerIP]	Defines the IP address of the Session Experience Manager (SEM) server. Note: For this parameter to take effect, a device reset is required.
[QOEPort]	Defines the port of the SEM server. The valid value range is 0 to 65534. The default is 5000.
[QOEInterfaceName]	Defines the IP network interface on which the quality experience reports are sent. The default is "DEFAULT". Note: For this parameter to take effect, a device reset is required
[QOEUseMosLQ]	Enables the reporting of the MOS-LQ (listening quality). If disabled, the MOS-CQ (conversational quality) is reported. MOS-LQ measures the quality of audio for listening purposes only. MOS-LQ does not take into account bi-directional effects such as delay and echo. MOS-CQ takes into account listening quality in both directions, as well as the bi-directional effects. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable

Parameter	Description
Media Realm > Quality of Experience Table	
Web: Media Realm > Quality Of Experience [QOERules]	This table configures Quality of Experience parameters per Media Realm. [QOERules] FORMAT QOERules_Index = QOERules_MediaRealmIndex, QOERules_RuleIndex, QOERules_MonitoredParam, QOERules_Profile, QOERules_GreenYellowThreshold, QOERules_GreenYellowHystersis, QOERules_YellowRedThreshold, QOERules_YellowRedHystersis; [\QOERules]

A.8 Control Network Parameters

A.8.1 IP Group, Proxy, Registration and Authentication Parameters

The proxy server, registration and authentication SIP parameters are described in the table below.

Table A-29: Proxy, Registration and Authentication SIP Parameters

Parameter	Description
IP Group Table	
Web: IP Group Table EMS: Endpoints > IP Group [IPGroup]	This <i>parameter</i> table 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_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList, IPGroup_EnableSBCCClientForking, IPGroup_ContactName; [/IPGroup] For example: IPGroup 1 = 0, "dol gateway", 1, firstIPgroup, , 0, -1, 0, 0, -1, 0, mrealm1, 1, 1, ; IPGroup 2 = 0, "abc server", 2, secondIPgroup, , 0, -1, 0, 0, -1, 0, mrealm2, 1, 2, ; IPGroup 3 = 1, "IP phones", 1, thirdIPGroup, , 0, -1, 0, 0, -1, 0, mrealm3, 1, 2, ; Notes: <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ This table parameter can include up to 32 indices (where 1 is the first index). ▪ The parameters Type, RoutingMode, EnableSurvivability, ServingIPGroup, SRD, and ClassifyByProxySet are not applicable to

Parameter	Description
	Mediant 600. <ul style="list-style-type: none"> ▪ For a detailed description of the <i>ini</i> file table's parameters and for configuring this table using the Web interface, see 'Configuring IP Groups' on page 193. ▪ For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Web: Authentication Table EMS: SIP Endpoints > Authentication	
[Authentication]	This parameter table 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_Module, Authentication_Port; [Authentication] Where, <ul style="list-style-type: none"> ▪ UserId = User name ▪ UserPassword = Password ▪ Module = Module number (where 1 depicts the module in Slot 1) ▪ Port = Port number (where 1 depicts the Port 1 of the module) For example: Authentication 0 = john,1325,1,1; (user name "john" with password 1325 for authenticating Port 1 of Module 1) Authentication 1 = lee,1552,1,2; (user name "lee" with password 1552 for authenticating Port 2 of Module 1) Notes: <ul style="list-style-type: none"> ▪ The indexing of this parameter starts at 0. ▪ 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 are not configured, the port's phone number (configured using the parameter TrunkGroup - Trunk Group 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 316. ▪ For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Account Table	
Web: Account Table EMS: SIP Endpoints > Account [Account]	This <i>parameter</i> table configures the Account table for registering and/or authenticating (digest) Trunk Groups or IP 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;

Parameter	Description
	<p>[Account]</p> <p>For example: Account 1 = 1, -1, 1, user, 1234, acl, 1, ITSP1;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table can include up to 32 indices (where 1 is the first index). ▪ The parameter Account_ApplicationType 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 Trunk Group or IP 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 223. ▪ For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Proxy Registration Parameters	
<p>Web: Use Default Proxy EMS: Proxy Used [IsProxyUsed]</p>	<p>Enables the use of a SIP proxy server.</p> <ul style="list-style-type: none"> ▪ [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 198). <p>Note: If you are not using a proxy server, you must define outbound IP call routing rules in the Outbound IP Routing Table' (described in 'Configuring Outbound IP Routing Table' on page 269).</p>
<p>Web/EMS: Proxy Name [ProxyName]</p>	<p>Defines the Home Proxy domain name. If specified, this name is used as the Request-URI in REGISTER, INVITE, and other SIP messages, and as the host part of the To header in INVITE messages. If not specified, the Proxy IP address is used instead. The value must be string of up to 49 characters.</p>
<p>Web: Redundancy Mode EMS: Proxy Redundancy Mode [ProxyRedundancyMode]</p>	<p>Determines whether the device switches back to the primary Proxy after using a redundant Proxy.</p> <ul style="list-style-type: none"> ▪ [0] Parking = device continues working with a redundant (now active) Proxy until the next failure, after which it works 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). <p>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.</p>
<p>Web: Proxy IP List Refresh Time EMS: IP List Refresh Time [ProxyIPListRefreshTime]</p>	<p>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.</p>
<p>Web: Enable Fallback to Routing Table EMS: Fallback Used</p>	<p>Determines whether the device falls back to the Outbound IP Routing Table' for call routing when Proxy servers are unavailable.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Fallback is not used (default).

Parameter	Description
[IsFallbackUsed]	<ul style="list-style-type: none"> ▪ [1] Enable = The Outbound IP Routing Table' is used when Proxy servers are unavailable. <p>When the device falls back to the Outbound IP Routing Table', it continues scanning for a Proxy. When the device locates an active Proxy, it switches from internal routing back to Proxy routing.</p> <p>Note: To enable the redundant Proxies mechanism, set the parameter EnableProxyKeepAlive to 1 or 2.</p>
Web/EMS: Prefer Routing Table [PreferRouteTable]	<p>Determines whether the device's internal routing table takes precedence over a Proxy for routing calls.</p> <ul style="list-style-type: none"> ▪ [0] No = Only a Proxy server is used to route calls (default). ▪ [1] Yes = The device checks the routing rules in the Outbound IP Routing Table' for a match with the Tel-to-IP call. Only if a match is not found is a Proxy used.
Web/EMS: Always Use Proxy [AlwaysSendToProxy]	<p>Determines whether the device sends SIP messages and responses through a Proxy server.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Use standard SIP routing rules (default). ▪ [1] Enable = All SIP messages and responses are sent to the Proxy server. <p>Note: This parameter is applicable only if a Proxy server is used (i.e., the parameter IsProxyUsed is set to 1).</p>
Web: SIP ReRouting Mode EMS: SIP Re-Routing Mode [SIPreroutingMode]	<p>Determines the routing mode after a call redirection (i.e., a 3xx SIP response is received) or transfer (i.e., a SIP REFER request is received).</p> <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 redirect calls. ▪ This parameter is disregarded if the parameter AlwaysSendToProxy is set to 1.
Web/EMS: DNS Query Type [DNSQueryType]	<p>Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to resolve Proxy and Registrar servers and to resolve all domain names that appear in the SIP Contact and Record-Route headers.</p> <ul style="list-style-type: none"> ▪ [0] A-Record (default) ▪ [1] SRV ▪ [2] NAPTR

Parameter	Description
	<p>If set to A-Record [0], no NAPTR or SRV queries are performed.</p> <p>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.</p> <p>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.</p> <p>If the Proxy/Registrar IP address parameter, the domain name in the Contact/Record-Route headers, or the IP address defined in the Routing tables contain a domain name with port definition, the device performs a regular DNS A-record query.</p> <p>If a specific Transport Type is defined, a NAPTR query is not performed. Note: To enable NAPTR/SRV queries for Proxy servers only, use the parameter ProxyDNSQueryType.</p>
<p>Web: Proxy DNS Query Type [ProxyDNSQueryType]</p>	<p>Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to discover Proxy servers.</p> <ul style="list-style-type: none"> ▪ [0] A-Record (default) ▪ [1] SRV ▪ [2] NAPTR <p>If set to A-Record [0], no NAPTR or SRV queries are performed.</p> <p>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 returns two domain names and the A-record queries return two IP addresses each, no additional searches are performed.</p> <p>If set to NAPTR [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.</p> <p>If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = domain.com:5080), the device performs a regular DNS A-record query.</p> <p>If a specific Transport Type is defined, a NAPTR query is not performed. Note: When enabled, NAPTR/SRV queries are used to discover Proxy servers even if the parameter DNSQueryType is disabled.</p>
<p>Web/EMS: Graceful Busy Out Timeout [sec] [GracefulBusyOutTimeout]</p>	<p>Defines the timeout interval (in seconds) for Out of Service (OOS) graceful shutdown mode for busy trunks (per trunk) if communication fails with a Proxy server (or Proxy Set). In such a scenario, the device rejects new calls from the PSTN (Serving Trunk Group), but maintains currently active calls for this user-defined timeout. Once this timeout elapses, the device terminates currently active calls and takes the trunk out of service (sending the PSTN busy-out signal). Trunks on which no calls are active are immediately taken out of service regardless of the timeout.</p> <p>The range is 0 to 3,600. The default is 0.</p>

Parameter	Description
	Note: This parameter is applicable only to digital interfaces.
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. <ul style="list-style-type: none"> ▪ [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]	Defines the user name used for registration and Basic/Digest authentication with a Proxy/Registrar server. The default value is an empty string. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 316).
Web/EMS: Password [Password]	Defines the password for Basic/Digest authentication with a Proxy/Registrar server. A single password is used for all device ports. The default is 'Default_Passwd'. <p>Note: Instead of configuring this parameter, the Authentication table can be used (see Authentication on page 316).</p>
Web/EMS: Cnonce [Cnonce]	Defines the 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'.
Web/EMS: Mutual Authentication Mode [MutualAuthenticationMode]	Determines the device's mode of operation when Authentication and Key Agreement (AKA) Digest Authentication is used. <ul style="list-style-type: none"> ▪ [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. <ul style="list-style-type: none"> ▪ [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 mixture of REGISTER and INVITE authorizations.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [2] Full = Caches all challenges from the proxies. <p>Note: Challenge Caching is used with all proxies and not only with the active one.</p>
Proxy IP Table	
Web: Proxy IP Table EMS: Proxy IP [ProxyIP]	<p>This <i>parameter</i> table configures the Proxy Set table with Proxy Set IDs, each with up to five Proxy server IP addresses (or fully qualified domain name/FQDN). Each Proxy Set can be defined with a transport type (UDP, TCP, or TLS). The format of this parameter is as follows:</p> <pre>[ProxyIP] FORMAT ProxyIp_Index = ProxyIp_IpAddress, ProxyIp_TransportType, ProxyIp_ProxySetId; [\ProxyIP]</pre> <p>For example: ProxyIp 0 = 10.33.37.77, -1, 0; ProxyIp 1 = 10.8.8.10, 0, 2; ProxyIp 2 = 10.5.6.7, -1, 1;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 <i>ini</i> file table, see 'Configuring Proxy Sets Table' on page 198. ▪ For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Proxy Set Table	
Web: Proxy Set Table EMS: Proxy Set [ProxySet]	<p>This <i>parameter</i> table configures the Proxy Set ID table. It is used in conjunction with the ProxyIP <i>ini</i> file table parameter, which defines the IP addresses per Proxy Set ID.</p> <p>The ProxySet <i>ini</i> 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).</p> <p>The format of this parameter is as follows:</p> <pre>[ProxySet] FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRD, ProxySet_ClassificationInput, ProxySet_ProxyRedundancyMode; [\ProxySet]</pre> <p>For example: ProxySet 0 = 0, 60, 0, 0, 0, , 1; ProxySet 1 = 1, 60, 1, 0, 1, , 0;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table parameter can include up to 32 indices (0-31). ▪ For configuring the Proxy Set IDs and their IP addresses, use the parameter ProxyIP. ▪ The parameter ProxySet_ClassificationInput is not applicable. ▪ For configuring the Proxy Set ID table using the Web interface and for a detailed description of the parameters of this <i>ini</i> file table, see

Parameter	Description
	'Configuring Proxy Sets Table' on page 198. <ul style="list-style-type: none"> For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Registrar Parameters	
Web: Enable Registration EMS: Is Register Needed [IsRegisterNeeded]	Enables the device to register to a Proxy/Registrar server. <ul style="list-style-type: none"> [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). <p>Note: The device sends a REGISTER request for each channel or for the entire device (according to the AuthenticationMode parameter).</p>
Web/EMS: Registrar Name [RegistrarName]	Defines the 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 100 characters.
Web: Registrar IP Address EMS: Registrar IP [RegistrarIP]	Defines the IP address (or FQDN) and port number (optional) of the Registrar server. The IP address is in dotted-decimal notation, e.g., 201.10.8.1:<5080>. <p>Notes:</p> <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> [-1] Not Configured (default) [0] UDP [1] TCP [2] TLS <p>Note: When set to 'Not Configured', the value of the parameter SIPTransportType is used.</p>
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.

Parameter	Description
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.
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. <ul style="list-style-type: none"> ▪ [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: <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable

Parameter	Description
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.
Web/EMS: Registration Mode [AuthenticationMode]	Determines the device's registration and authentication method. <ul style="list-style-type: none"> ▪ [0] Per Endpoint = Registration and authentication is performed separately for each endpoint/B-channel. This is typically used for FXS interfaces, where each endpoint registers (and authenticates) separately with its user name and password. ▪ [1] Per Gateway = Single registration and authentication for the entire device (default). This is typically used for FXO interfaces and digital modules. ▪ [3] Per FXS = Registration and authentication for FXS endpoints.
Web: Set Out-Of-Service On Registration Failure EMS: Set OOS On Registration Fail [OOSOnRegistrationFail]	Enables setting an endpoint, trunk, or the entire device (i.e., all endpoints) to out-of-service if registration fails. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable If the registration is per endpoint (i.e., AuthenticationMode is set to 0) or per Account (see 'Configuring Trunk Group Settings' on page 251) and a specific endpoint/Account registration fails (SIP 4xx or no response), then that endpoint is set to out-of-service until a success response is received in a subsequent registration request. When the registration is per the entire device (i.e., AuthenticationMode is set to 1) and registration fails, all endpoints are set to out-of-service. If all the Accounts of a specific Trunk Group fail registration and if the Trunk Group comprises a complete trunk, then the entire trunk is set to out-of-service. Note: The out-of-service method is configured using the parameter FXSOOSBehavior.
[UnregistrationMode]	Enables the device to perform explicit unregisters. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable = The device sends an asterisk ("*") value in the SIP Contact header, instructing the Registrar server to remove all previous registration bindings. The device removes SIP User Agent (UA) registration bindings in a Registrar, according to RFC 3261. Registrations are soft state and expire unless refreshed, but they can also be explicitly removed. A client can attempt to influence the expiration interval selected by the Registrar. A UA requests the immediate removal of a binding by specifying an expiration interval of "0" for that contact address in a REGISTER request. UA's should support this mechanism so that bindings can be removed before their expiration interval has passed. Use of the "*" Contact header field value allows a registering UA to remove all bindings associated with an address-of-record (AOR) without knowing their precise values. 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".
Web/EMS: Add Empty	Enables the inclusion of the SIP Authorization header in initial

Parameter	Description
Authorization Header [EmptyAuthorizationHeader]	<p>registration (REGISTER) requests sent by the device.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>The Authorization header carries the credentials of a user agent (UA) in a request to a server. The sent REGISTER message populates the Authorization header with the following parameters:</p> <ul style="list-style-type: none"> ▪ username - set to the value of the private user identity ▪ realm - set to the domain name of the home network ▪ uri - set to the SIP URI of the domain name of the home network ▪ nonce - set to an empty value ▪ response - set to an empty value <p>For example:</p> <pre>Authorization: Digest username=alice_private@home1.net, realm="home1.net", nonce="", response="e56131d19580cd833064787ecc"</pre> <p>Note: This registration header is according to the IMS 3GPP TS24.229 and PKT-SP-24.220 specifications.</p>
Web: Add initial Route Header [InitialRouteHeader]	<p>Enables the inclusion of the SIP Route header in initial registration or re-registration (REGISTER) requests sent by the device.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>When the device sends a REGISTER message, the Route header includes either the Proxy's FQDN, or IP address and port according to the configured Proxy Set, for example:</p> <pre>Route: <sip:10.10.10.10;lr;transport=udp></pre> <p>or</p> <pre>Route: <sip: pcscf-gm.ims.rr.com;lr;transport=udp></pre>
[UsePingPongKeepAlive]	<p>Enables the use of the carriage-return and line-feed sequences (CRLF) Keep-Alive mechanism, according to RFC 5626 "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)" for reliable, connection-orientated transport types such as TCP.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>The SIP user agent/client (i.e., device) uses a simple periodic message as a keep-alive mechanism to keep their flow to the proxy or registrar alive (used for example, to keep NAT bindings open). For connection-oriented transports such as TCP/TLS this is based on CRLF. This mechanism uses a client-to-server "ping" keep-alive and a corresponding server-to-client "pong" message. This ping-pong sequence allows the client, and optionally the server, to tell if its flow is still active and useful for SIP traffic. If the client does not receive a pong in response to its ping, it declares the flow "dead" and opens a new flow in its place. In the CRLF Keep-Alive mechanism the client periodically (defined by the PingPongKeepAliveTime parameter) sends a double-CRLF (the "ping") then waits to receive a single CRLF (the "pong"). If the client does not receive a "pong" within an appropriate amount of time, it considers the flow failed.</p> <p>Note: The device sends a CRLF message to the Proxy Set only if the Proxy Keep-Alive feature (EnableProxyKeepAlive parameter) is enabled</p>

Parameter	Description
	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]	<p>Defines the periodic interval (in seconds) after which a “ping” (double-CRLF) keep-alive is sent to a proxy/registrar, using the CRLF Keep-Alive mechanism.</p> <p>The default range is 5 to 2,000,000. The default is 120.</p> <p>The device uses the range of 80-100% of this user-defined value as the actual interval. For example, if the parameter value is set to 200 sec, the interval used is any random time between 160 to 200 seconds. This prevents an “avalanche” of keep-alive by multiple SIP UAs to a specific server.</p>

A.8.2 Network Application Parameters

The SIP network application parameters are described in the table below.

Table A-30: SIP Network Application Parameters

Parameter	Description
Signaling Routing Domain Table	
Web: SRD Settings EMS: SRD Table [SRD]	<p>This <i>parameter</i> table configures the Signaling Routing Domain (SRD) table. The format of this parameter is as follows:</p> <pre>[SRD] FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations; [SRD]</pre> <p>For example: SRD 1 = LAN1_SRD, Mrealm1, 0, 1, 15, 1; SRD 2 = LAN2_SRD, Mrealm2, 0, 1, 15, 1;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table can include up to 32 indices (where 0 is the first index). ▪ The following parameters are not applicable: IntraSRDMediaAnchoring, BlockUnRegUsers, MaxNumOfRegUsers, and EnableUnAuthenticatedRegistrations. ▪ For a detailed description of the table's individual parameters and for configuring the table using the Web interface, see 'Configuring SRD Table' on page 189. ▪ For a description on configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
SIP Interface Table	
Web: SIP Interface Table EMS: SIP Interfaces Table [SIPInterface]	<p>This <i>parameter</i> table configures the SIP Interface table. The SIP Interface represents a SIP signaling entity, comprising ports (UDP, TCP, and TLS) and associated with a specific IP interface and an SRD ID. The format of this parameter is as follows:</p> <pre>[SIPInterface] FORMAT SIPInterface_Index = SIPInterface_NetworkInterface, SIPInterface_ApplicationType, SIPInterface_UDPPort,</pre>

Parameter	Description
	<p>SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRD; [\SIPInterface]</p> <p>For example: SIPInterface 0 = Voice, 2, 5060, 5060, 5061, 1; SIPInterface 1 = Voice, 2, 5070, 5070, 5071, 2; SIPInterface 2 = Voice, 0, 5090, 5000, 5081, 2;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table can include up to 32 indices (where 0 is the first index). ▪ Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping). ▪ You can define up to two different SIP Interfaces per SRD, where each SIP Interface pertains to a different application type (i.e., GW, SAS). ▪ For a detailed description of the table's individual parameters and for configuring the table using the Web interface, see 'Configuring SIP Interface Table' on page 191. ▪ For a description on configuring <i>ini</i> file table parameters, see 'Format of ini File Table Parameters' on page 84.
NAT Translation Table	
<p>Web: NAT Translation Table [NATtranslation]</p>	<p>This <i>parameter</i> table defines NAT rules for translating source IP addresses per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses. This allows, for example, the separation of VoIP traffic between different ISTRP's, and topology hiding (of internal IP addresses to the "public" network). Each IP interface (configured in the Multiple Interface table - InterfaceTable parameter) can be associated with a NAT rule in this table, translating the source IP address and port of the outgoing packet into the NAT address (IP address and port range). The format of this parameter is as follows:</p> <pre>[NATtranslation] FORMAT NATtranslation_Index = NATtranslation_SourceIPInterfaceName, NATtranslation_TargetIPAddress, NATtranslation_SourceStartPort, NATtranslation_SourceEndPort, NATtranslation_TargetStartPort, NATtranslation_TargetEndPort; [\NATtranslation]</pre> <p>Where:</p> <ul style="list-style-type: none"> ▪ SourceIPInterfaceName = name of the IP interface as defined in the Multiple Interface table. ▪ TargetIPAddress = global IP address. ▪ TargetStartPort and TargetEndPort = (optional) port range (1-65536) of the global address. If no ports are required, leave this field blank. ▪ SourceStartPort and SourceEndPort = (optional) port range (1-65536) of the IP interface. If no ports are required, leave this field blank. <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table can include up to 32 indices. ▪ If the Multiple Interface table (InterfaceTable parameter) is not configured, the default SourceIPInterfaceName is "All". This represents the single IP interface for OAMP, Control, and Media (defined by the LocalOAMIPAddress, LocalOAMSubnetMask, and LocalOAMDefaultGW parameters). ▪ The device's priority method for performing NAT is as follows:

Parameter	Description
	<ul style="list-style-type: none"> a. Uses an external STUN server (STUNServerPrimaryIP parameter) to assign a NAT address for all interfaces. b. Uses the StaticNATIP parameter to define one NAT IP address for all interfaces. c. Uses the NATTranslation parameter to define NAT per interface. ▪ If NAT is not configured (by any of the above-mentioned methods), the device sends the packet according to its IP address defined in the Multiple Interface table.

A.9 General SIP Parameters

The general SIP parameters are described in the table below.

Table A-31: 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. <ul style="list-style-type: none"> ▪ [0] (default) = Disabled - the device sends the SIP response to the UDP port defined in the Via header. If the Via header contains the 'rport' parameter, the response is sent to the UDP port from where the SIP request is received. ▪ [1] = Enabled - SIP responses are sent to the UDP port from where SIP requests are received even if the 'rport' parameter is not present in the Via header.
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]	Defines the maximum number of concurrent calls per IP Profile. If the IP Profile is set to some limit, the device maintains the number of concurrent calls (incoming and outgoing) pertaining to the specific profile. When the number of concurrent calls is equal to the limit, the device rejects any new incoming and outgoing calls belonging to that profile. This parameter can also be set to the following: <ul style="list-style-type: none"> ▪ [-1] = There is no limitation on calls for that IP Profile (default). ▪ [0] = Calls are rejected. Notes: <ul style="list-style-type: none"> ▪ This parameter can only be configured for an IP Profile using the IPProfile parameter (see 'Configuring IP Profiles' on page 217). ▪ For IP-to-IP calls, you can configure the device to route calls to an alternative IP Group when the maximum number of concurrent calls is reached. To do so, you need to add an alternative routing

Parameter	Description
Web: QoS statistics in SIP Release Call [QoSStatistics]	<p>rule in the Outbound IP Routing table that reroutes the call to an alternative IP Group. You also need to add a rule to the Reason for Alternative Routing table to initiate an alternative rule for Tel-to-IP calls using cause 805.</p> <p>Enables the device to include call quality of service (QoS) statistics in SIP BYE and SIP 200 OK response to BYE, using the proprietary SIP header X-RTP-Stat.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable <p>The X-RTP-Stat header provides the following statistics:</p> <ul style="list-style-type: none"> ▪ Number of received and sent voice packets ▪ Number of received and sent voice octets ▪ Received packet loss, jitter (in ms), and latency (in ms) <p>The X-RTP-Stat header contains the following fields:</p> <ul style="list-style-type: none"> ▪ PS=<voice packets sent> ▪ OS=<voice octets sent> ▪ PR=<voice packets received> ▪ OR=<voice octets received> ▪ PL=<receive packet loss> ▪ JI=<jitter in ms> ▪ LA=<latency in ms> <p>Below is an example of the X-RTP-Stat header in a SIP BYE message:</p> <pre> BYE sip:302@10.33.4.125 SIP/2.0 Via: SIP/2.0/UDP 10.33.4.126;branch=z9hG4bKac2127550866 Max-Forwards: 70 From: <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,PRA CK,REFER,INFO,SUBSCRIBE,UPDATE User-Agent: Sip-Gateway-/v.6.2A.008.006 Reason: Q.850 ;cause=16 ;text="local" Content-Length: 0 </pre>
Web/EMS: PRACK Mode [PrackMode]	<p>Determines the PRACK (Provisional Acknowledgment) mechanism mode for SIP 1xx reliable responses.</p> <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Supported (default) ▪ [2] Required <p>Notes:</p>

Parameter	Description
Web/EMS: Enable Early Media [EnableEarlyMedia]	<ul style="list-style-type: none"> ▪ The Supported and Required headers contain the '100rel' tag. ▪ The device sends PRACK messages if 180/183 responses are received with '100rel' in the Supported or Required headers. <p>Digital: Enables the device to send a 18x response with SDP instead of a 18x, allowing the media stream to be established prior to the answering of the call.</p> <p>Analog: Enables the device to send a 183 Session Progress response with SDP instead of a 180 Ringing, allowing the media stream to be established prior to the answering of the call.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Early Media is disabled (default). ▪ [1] Enable = Enables Early Media. <p>Digital: The inclusion of the SDP in the 18x response depends on the ISDN Progress Indicator (PI). The SDP is sent only if PI is set to 1 or 8 in the received Proceeding, Alerting, or Progress PRI messages. See also the ProgressIndicator2IP parameter, which if set to 1 or 8, the device behaves as if it received the ISDN messages with the PI.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ See also the IgnoreAlertAfterEarlyMedia parameter. This parameter allows, for example, to interwork Alert + PI to SIP 183 + SDP instead of 180 + SDP. ▪ You can also configure early SIP 183 response immediately upon receipt of an INVITE, using the EnableEarly183 parameter. ▪ Analog: To send a 183 response, you must also set the parameter ProgressIndicator2IP to 1. If it is equal to 0, 180 Ringing response is sent. ▪ This parameter can be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 217) and per Tel profile, using the TelProfile parameter (see 'Configuring Tel Profiles' on page 215).
Web/EMS: Enable Early 183 [EnableEarly183]	<p>Enables the device to send SIP 183 responses with SDP to the IP upon receipt of INVITE messages (for IP-to-Tel calls). The device sends the RTP packets only once it receives an ISDN Progress, Alerting with Progress indicator, or Connect message from the PSTN.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>For example, if enabled and the device receives an ISDN Progress message, it starts sending RTP packets according to the initial negotiation without sending the 183 response again. Therefore, this feature reduces clipping of early media.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ To enable this feature, configure the EnableEarlyMedia parameter to 1. ▪ This feature is applicable only to ISDN interfaces.
[IgnoreAlertAfterEarlyMedia]	<p>Determines the device's interworking of Alerting messages from PRI to SIP.</p> <ul style="list-style-type: none"> ▪ [0] = Disabled (default) ▪ [1] = Enabled <p>When enabled, if the device sends a 183 response with an SDP (due to a received ISDN Progress or Proceeding with PI messages) and an Alerting message is then received from the Tel side (with or without Progress Indicator), the device does not send an additional 18x response, and the voice channel remains open. However, if the</p>

Parameter	Description
	<p>device did not send a 183 with an SDP and it receives an Alert without PI, the device sends a 180 (without SDP). If it receives an Alert with PI it sends a 183with an SDP.</p> <p>When disabled, the device sends additional 18x responses as a result of receiving Alerting and Progress messages, regardless of whether or not a 18x response was already sent.</p> <p>Note: This parameter is applicable only if the EnableEarlyMedia parameter is set to 1 (i.e., enabled).</p>
Web: 183 Message Behavior EMS: SIP 183 Behaviour [SIP183Behaviour]	<p>Digital interfaces: Defines the ISDN message that is sent when the 183 Session Progress message is received for IP-to-Tel calls. Analog interfaces: Defines the response of the device upon receipt of a SIP 183 response.</p> <ul style="list-style-type: none"> ▪ [0] Progress = Digital interfaces: The device sends a Progress message. Analog interfaces: A 183 response (without SDP) does not cause the device to play a ringback tone (default). ▪ [1] Alert = Digital interfaces: The device sends an Alerting message (upon receipt of a 183 response) instead of an ISDN Progress message. Analog interfaces: 183 response is handled by the device as if a 180 Ringing response is received, and the device plays a ringback tone.
[ReleaseIP2ISDNCallOnProgressWithCause]	<p>Typically, if an Q.931 Progress message with a Cause is received from the PSTN for an outgoing IP-to-ISDN call and the EnableEarlyMedia parameter is set to 1 (i.e., the Early Media feature is enabled), the device interworks the Progress to 183+sdp to enable the originating party to hear the PSTN announcement about the call failure. Conversely, if EnableEarlyMedia is set to 0, the device disconnects the call by sending a SIP 4xx response to the originating party.</p> <p>However, if the ReleaseIP2ISDNCallOnProgressWithCause parameter is set to 1, the device sends a SIP 4xx response even if the EnableEarlyMedia parameter is set to 1.</p> <ul style="list-style-type: none"> ▪ [0] = If a Progress with Cause message is received from the PSTN for an outgoing IP-to-ISDN call, the device does not disconnect the call by sending a SIP 4xx response to the originating party (default). ▪ [1] = The device sends a SIP 4xx response when the EnableEarlyMedia parameter is set to 0. ▪ [2] = The device always sends a SIP 4xx response, even if the EnableEarlyMedia parameter is set to 1.
Web: Session-Expires Time EMS: Sip Session Expires [SIPSessionExpires]	<p>Defines the numerical value 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).</p>
Web: Minimum Session-Expires EMS: Minimal Session Refresh Value [MinSE]	<p>Defines the time (in seconds) that is used in the Min-SE header. This header defines the minimum time that the user agent refreshes the session. The valid range is 10 to 100,000. The default value is 90.</p>
Web/EMS: Session Expires Method [SessionExpiresMethod]	<p>Determines the SIP method used for session-timer updates.</p> <ul style="list-style-type: none"> ▪ [0] Re-INVITE = Uses Re-INVITE messages for session-timer updates (default).

Parameter	Description
	<ul style="list-style-type: none"> ▪ [1] UPDATE = Uses UPDATE messages. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> ▪ [0] = Do not remove tag (default). ▪ [1] = Remove tag.
[EnableRTCPAttribute]	Enables the use of the 'rtcp' attribute in the outgoing SDP. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable
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 (analog interfaces) or configuration parameter 'Username' value (digital interfaces) 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: TDM Over IP Minimum Calls For Trunk Activation EMS: TDM Over IP Min Calls For Trunk Activation [TDMOverIPMinCallsForTrunkActivation]	Defines the minimal number of SIP dialogs that must be established when using TDM Tunneling to consider the specific trunk as active. When using TDM Tunneling, if calls from this defined number of B-channels pertaining to a specific Trunk fail (i.e., SIP dialogs are not correctly set up), an AIS alarm is sent on this trunk toward the PSTN and all current calls are dropped. The originator gateway continues the INVITE attempts. When this number of calls succeed (i.e., SIP dialogs are correctly set up), the AIS alarm is cleared. The valid range is 0 to 31. The default value is 0 (i.e., don't send AIS alarms).
[TDMoIPInitiateInviteTime]	Defines the time (in msec) between the first INVITE issued within the same trunk when implementing the TDM tunneling application. The valid value range is 500 to 1000. The default is 500.
[TDMoIPInviteRetryTime]	Defines the time (in msec) between call release and a new INVITE when implementing the TDM tunneling application. The valid value range is 10,000 to 20,000. The default is 10,000.
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. <ul style="list-style-type: none"> ▪ [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). <p>Notes:</p> <ul style="list-style-type: none"> ▪ Fax adaptations (for options 2 and 3): <ul style="list-style-type: none"> ✓ Echo Celler = On

Parameter	Description
	<ul style="list-style-type: none"> ✓ 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 'gpmid' attribute is added to the SDP in the following format: <ul style="list-style-type: none"> ✓ For A-law: 'a=gpmid:8 vbd=yes;ecan=on' ✓ For μ-law: 'a=gpmid:0 vbd=yes;ecan=on' ▪ 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 more information on fax transport methods, see 'Fax/Modem Transport Modes' on page 144.
[HandleG711asVBD]	<p>Enables the handling of G.711 as G.711 VBD coder.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default). The device negotiates G.711 as a regular audio coder and sends an answer only with G.729 coder. For example, if the device is configured with G.729 and G.711 VBD coders and it receives an INVITE with an SDP offer containing G.729 and "regular" G.711 coders, it sends an SDP answer containing only the G.729 coder. ▪ [1] = Enable. The device assumes that the G.711 coder received in the INVITE SDP offer is a VBD coder. For example, if the device is configured with G.729 and G.711 VBD coders and it receives an INVITE with an SDP offer containing G.729 and "regular" G.711 coders, it sends an SDP answer containing G.729 and G.711 VBD coders, allowing a subsequent bypass (passthrough) session if fax/modem signals are detected during the call. <p>Note: This parameter is applicable only if G.711 VBD coder(s) are selected for the device (using the CodersGroup parameter).</p>
[FaxVBDBehavior]	<p>Determines the device's fax transport behavior when G.711 VBD coder is negotiated at call start.</p> <ul style="list-style-type: none"> ▪ [0] = If the device is configured with a VBD coder (see the CodersGroup parameter) and is negotiated OK at call start, then both fax and modem signals are sent over RTP using the bypass payload type (and no mid-call VBD or T.38 Re-INVITES occur). (Default.) ▪ [1] = If the IsFaxUsed parameter is set to 1, the channel opens with the FaxTransportMode parameter set to 1 (relay). This is required to detect mid-call fax tones and to send T.38 Re-INVITE messages upon fax detection. If the remote party supports T.38, the fax is relayed over T.38. <p>Notes:</p> <ul style="list-style-type: none"> ▪ If VBD coder negotiation fails at call start and if the IsFaxUsed parameter is set to 1 (or 3), then the channel opens with the FaxTransportMode parameter set to 1 (relay) to allow future detection of fax tones and sending of T.38 Re-INVITES. In such a scenario, the FaxVBDBehavior parameter has no effect.

Parameter	Description
	<ul style="list-style-type: none"> This feature can be used only if the remote party supports T.38 fax relay; otherwise, the fax fails.
Web: SIP Transport Type EMS: Transport Type [SIPTransportType]	Determines the default transport layer for outgoing SIP calls initiated by the device. <ul style="list-style-type: none"> [0] UDP (default) [1] TCP [2] TLS (SIPS) Notes: <ul style="list-style-type: none"> It's recommended to use TLS for communication with a SIP Proxy and not for direct device-to-device communication. For received calls (i.e., incoming), the device accepts all these protocols. 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 100 simultaneous TLS sessions.
Web: SIP UDP Local Port EMS: Local SIP Port [LocalSIPPort]	Defines the 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]	Defines the 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 [TLSTLocalSIPPort]	Defines the 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. <ul style="list-style-type: none"> [0] Disable (default). [1] Enable. When the SIPTransportType parameter is set to 2 (i.e., TLS) and the parameter EnableSIPS is disabled, TLS is used for the next network hop only. When the parameter SIPTransportType is set to 2 or 1 (i.e., TCP or TLS) and EnableSIPS is enabled, TLS is used through the entire connection (over multiple hops). 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. <ul style="list-style-type: none"> [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 [ReliableConnectionPersistentMode]	Enables setting of all TCP/TLS connections as persistent and therefore, not released. <ul style="list-style-type: none"> [0] = Disable (default) - all TCP connections (except those that are set to a proxy IP) are released if not used by any SIP dialog\transaction. [1] = Enable - TCP connections to all destinations are persistent and not released unless the device reaches 70% of its maximum TCP resources. While trying to send a SIP message connection, reuse policy determines whether live connections to the specific destination are re-

Parameter	Description
	<p>used.</p> <p>Persistent TCP connection ensures less network traffic due to fewer setting up and tearing down of TCP connections and reduced latency on subsequent requests due to avoidance of initial TCP handshake. For TLS, persistent connection may reduce the number of costly TLS handshakes to establish security associations, in addition to the initial TCP connection set up.</p> <p>Note: If the destination is a Proxy server, the TCP/TLS connection is persistent regardless of the settings of this parameter.</p>
Web/EMS: TCP Timeout [SIPTCPTimeout]	<p>Defines the Timer B (INVITE transaction timeout timer) and Timer F (non-INVITE transaction timeout timer), as defined in RFC 3261, when the SIP Transport Type is TCP.</p> <p>The valid range is 0 to 40 sec. The default value is 64*SIPT1Rtx msec.</p>
Web: SIP Destination Port EMS: Destination Port [SIPDestinationPort]	<p>Defines the SIP destination port for sending initial SIP requests. The valid range is 1 to 65534. The default port is 5060.</p> <p>Note: SIP responses are sent to the port specified in the Via header.</p>
Web: Use user=phone in SIP URL EMS: Is User Phone [IsUserPhone]	<p>Determines whether the 'user=phone' string is added to the SIP URI and SIP To header.</p> <ul style="list-style-type: none"> ▪ [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]	<p>Determines whether the 'user=phone' string is added to the From and Contact SIP headers.</p> <ul style="list-style-type: none"> ▪ [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]	<p>Determines the format of the URI in the P-Asserted-Identity and P-Preferred-Identity headers.</p> <ul style="list-style-type: none"> ▪ [0] Disable = 'sip:' (default) ▪ [1] Enable = 'tel:'
Web: Tel to IP No Answer Timeout EMS: IP Alert Timeout [IPAlertTimeout]	<p>Defines the time (in seconds) that the device waits for a 200 OK response from the called party (IP side) after sending an INVITE message. If the timer expires, the call is released.</p> <p>The valid range is 0 to 3600. The default value is 180.</p>
Web: Enable Remote Party ID EMS: Enable RPI Header [EnableRPIheader]	<p>Enables Remote-Party-Identity headers for calling and called numbers for Tel-to-IP calls.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable = Remote-Party-Identity headers are generated in SIP INVITE messages for both called and calling numbers.
Web: Enable History-Info Header EMS: Enable History Info [EnableHistoryInfo]	<p>Enables usage of the History-Info header.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>User Agent Client (UAC) Behavior:</p> <ul style="list-style-type: none"> ▪ 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

Parameter	Description												
	<p>last entry, and concatenates a new destination to it (if an additional request is sent). The order of the reasons is as follows:</p> <ul style="list-style-type: none"> a. Q.850 Reason b. SIP Reason c. SIP Response code <ul style="list-style-type: none"> ▪ 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 border="1" data-bbox="568 548 1401 835"> <thead> <tr> <th>SIP Reason Code</th> <th>ISDN Redirecting Reason</th> </tr> </thead> <tbody> <tr> <td>302 - Moved Temporarily</td> <td>Call Forward Universal (CFU)</td> </tr> <tr> <td>408 - Request Timeout</td> <td rowspan="3">Call Forward No Answer (CFNA)</td> </tr> <tr> <td>480 - Temporarily Unavailable</td> </tr> <tr> <td>487 - Request Terminated</td> </tr> <tr> <td>486 - Busy Here</td> <td>Call Forward Busy (CFB)</td> </tr> <tr> <td>600 - Busy Everywhere</td> <td></td> </tr> </tbody> </table> <ul style="list-style-type: none"> ▪ 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. <p>User Agent Server (UAS) Behavior:</p> <ul style="list-style-type: none"> ▪ 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. 	SIP Reason Code	ISDN Redirecting Reason	302 - Moved Temporarily	Call Forward Universal (CFU)	408 - Request Timeout	Call Forward No Answer (CFNA)	480 - Temporarily Unavailable	487 - Request Terminated	486 - Busy Here	Call Forward Busy (CFB)	600 - Busy Everywhere	
SIP Reason Code	ISDN Redirecting Reason												
302 - Moved Temporarily	Call Forward Universal (CFU)												
408 - Request Timeout	Call Forward No Answer (CFNA)												
480 - Temporarily Unavailable													
487 - Request Terminated													
486 - Busy Here	Call Forward Busy (CFB)												
600 - Busy Everywhere													
Web: Use Tgrp Information EMS: Use SIP Tgrp [UseSIPtgrp]	<p>Determines whether the SIP 'tgrp' parameter is used. This SIP parameter specifies the Trunk Group to which the call belongs (according to RFC 4904). For example, the SIP message below indicates that the call belongs to Trunk Group ID 1:</p> <pre>INVITE sip::+16305550100;tgrp=1;trunk-context=example.com@10.1.0.3;user=phone SIP/2.0</pre> <ul style="list-style-type: none"> ▪ [0] Disable (default) = The 'tgrp' parameter isn't used. ▪ [1] Send Only = The Trunk Group number is added to the 'tgrp' parameter value in the Contact header of outgoing SIP messages. If a Trunk 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 call) contains "tgrp=<source trunk group ID>;trunk-context=<gateway IP address>". The <source trunk group ID> is the Trunk 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 Trunk Group ID used for outgoing Tel calls. The <gateway IP address> in "trunk-context" can be configured using the parameter SIPGatewayName. 												

Parameter	Description
	<ul style="list-style-type: none"> ▪ [3] Hotline = Interworks the hotline "Off Hook Indicator" parameter between SIP and ISDN: <ul style="list-style-type: none"> ✓ For IP-to-ISDN calls: <ul style="list-style-type: none"> - The device interworks the SIP tgrp=hotline parameter (received in INVITE) to ISDN Setup with the Off Hook Indicator IE of "Voice", and "Speech" Bearer Capability IE. Note that the Off Hook Indicator IE is described in UCR 2008 specifications. - The device interworks the SIP tgrp=hotline-ccdata parameter (received in INVITE) to ISDN Setup with an Off Hook Indicator IE of "Data", and with "Unrestricted 64k" Bearer Capability IE. The following is an example of the INVITE with tgrp=hotline-ccdata: <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;">INVITE sip:1234567;tgrp=hotline-ccdata;trunk-context=dsn.mil@example.com</div> ✓ For ISDN-to-IP calls: <ul style="list-style-type: none"> - The device interworks ISDN Setup with an Off Hook Indicator of "Voice" to SIP INVITE with "tgrp=hotline;trunk-context=dsn.mil" in the Contact header. - The device interworks ISDN Setup with an Off Hook indicator of "Data" to SIP INVITE with "tgrp=hotline-ccdata;trunk-context=dsn.mil" in the Contact header. - If ISDN Setup does not contain an Off Hook Indicator IE and the Bearer Capability IE contains "Unrestricted 64k", the outgoing INVITE includes "tgrp=ccdata;trunk-context=dsn.mil". If the Bearer Capability IE contains "Speech", the INVITE in this case does not contain tgrp and trunk-context parameters. ▪ [4] Hotline Extended = Interworks the ISDN Setup message's hotline "OffHook Indicator" Information Element (IE) to SIP INVITE's Request-URI and Contact headers. (Note: For IP-to-ISDN calls, the device handles the call as described in option [3].) <ul style="list-style-type: none"> ✓ The device interworks ISDN Setup with an Off Hook Indicator of "Voice" to SIP INVITE Request-URI and Contact header with "tgrp=hotline;trunk-context=dsn.mil". ✓ The device interworks ISDN Setup with an Off Hook indicator of "Data" to SIP INVITE Request-URI and Contact header with "tgrp=hotline-ccdata;trunk-context=dsn.mil". ✓ If ISDN Setup does not contain an Off Hook Indicator IE and the Bearer Capability IE contains "Unrestricted 64k", the outgoing INVITE Request-URI and Contact header includes "tgrp=ccdata;trunk-context=dsn.mil". If the Bearer Capability IE contains "Speech", the INVITE in this case does not contain tgrp and trunk-context parameters. <p>Note: IP-to-Tel configuration (using the PSTNPrefix parameter) overrides the 'tgrp' parameter in incoming INVITE messages.</p>
Web/EMS: TGRP Routing Precedence [TGRProuingPrecedence]	<p>Determines the precedence method for routing IP-to-Tel calls - according to the Inbound IP Routing Table' or according to the SIP 'tgrp' parameter.</p> <ul style="list-style-type: none"> ▪ [0] (default) = IP-to-Tel routing is determined by the Inbound IP Routing Table' (PSTNPrefix parameter). If a matching rule is not found in this table, the device uses the Trunk Group parameters for 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

Parameter	Description
	<p>contain the 'tgrp' parameter or if the Trunk Group number is not defined, then the Inbound IP Routing Table' is used for routing the call.</p> <p>Below is an example of an INVITE Request-URI with the 'tgrp' parameter, indicating that the IP call should be routed to Trunk Group 7:</p> <pre>INVITE sip:200;tgrp=7;trunk-context=example.com@10.33.2.68;user=phone SIP/2.0</pre> <p>Notes:</p> <ul style="list-style-type: none"> For enabling routing based on the 'tgrp' parameter, the UseSIPTrgrp 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]	<p>Determines whether the device uses the 'dtg' parameter for routing IP-to-Tel calls to a specific Trunk Group.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable <p>When this parameter is enabled, if the Request-URI in the received SIP INVITE includes the 'dtg' parameter, the device routes the call to the Trunk Group according to its value. This parameter is used instead of the 'tgrp/trunk-context' parameters. The dtg parameter appears in the INVITE Request-URI (and in the To header).</p> <p>For example, the received SIP message below routes the call to Trunk Group ID 56:</p> <pre>INVITE sip:123456@192.168.1.2;dtg=56;user=phone SIP/2.0</pre> <p>Note: If the Trunk Group is not found based on the 'dtg' parameter, the Inbound IP Routing Table' is used instead for routing the call to the appropriate Trunk Group.</p>
Web/EMS: Enable GRUU [EnableGRUU]	<p>Determines whether the Globally Routable User Agent URIs (GRUU) mechanism is used, according to RFC 5627. This is used for obtaining a GRUU from a registrar and for communicating a GRUU to a peer within a dialog.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable <p>A GRUU is a SIP URI that routes to an instance-specific UA and can be reachable from anywhere. There are a number of contexts in which it is desirable to have an identifier that addresses a single UA (using GRUU) rather than the group of UA's indicated by an Address of Record (AOR). For example, in call transfer where user A is talking to user B, and user A wants to transfer the call to user C. User A sends a REFER to user C:</p> <pre>REFER sip:C@domain.com SIP/2.0 From: sip:A@domain.com;tag=99asd To: sip:C@domain.com Refer-To: (URI that identifies B's UA)</pre> <p>The Refer-To header needs to contain a URI that user C can use to place a call to user B. This call needs to route to the specific UA instance that user B is using to talk to user A. User B should provide user A with a URI that has to be usable by anyone. It needs to be a GRUU.</p> <ul style="list-style-type: none"> Obtaining a GRUU: The mechanism for obtaining a GRUU is through registrations. A UA can obtain a GRUU by generating a

Parameter	Description
	<p>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:</p> <ul style="list-style-type: none"> ✓ If the REGISTER is per the device's client (endpoint), it is the MAC address concatenated with the phone number of the client. ✓ If the REGISTER is per device, it is the MAC address only. ✓ When using TP, "User Info" can be used for registering per endpoint. Thus, each endpoint can get a unique id – its phone number. The globally unique ID in TP is the MAC address concatenated with the phone number of the endpoint. <p>If the remote server doesn't support GRUU, it ignores the parameters of the GRUU. Otherwise, if the remote side also supports GRUU, the REGISTER responses contain the "gruu" parameter in each Contact header. This parameter contains a SIP or SIPS URI that represents a GRUU corresponding to the UA instance that registered the contact. The server provides the same GRUU for the same AOR and instance-id when sending REGISTER again after registration expiration. RFC 5627 specifies that the remote target is a GRUU target if its' Contact URL has the "gr" parameter with or without a value.</p> <ul style="list-style-type: none"> ▪ 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.
<p>EMS: Is CISCO Sce Mode [IsCiscoSCEMode]</p>	<p>Determines whether a Cisco gateway exists at the remote side.</p> <ul style="list-style-type: none"> ▪ [0] = No Cisco gateway exists at the remote side (default). ▪ [1] = A Cisco gateway exists at the remote side. <p>When a Cisco gateway exists at the remote side, the device must set the value of the 'annexb' parameter of the fntp attribute in the SDP to 'no'. This logic is used if the parameter EnableSilenceCompression is set to 2 (enable without adaptation). In this case, Silence Suppression is used on the channel but not declared in the SDP.</p> <p>Note: The IsCiscoSCEMode parameter is applicable only when the selected coder is G.729.</p>
<p>Web: User-Agent Information EMS: User Agent Display Info [UserAgentDisplayInfo]</p>	<p>Defines the string that is used in the SIP User-Agent and Server response headers. When configured, the string <UserAgentDisplayInfo value>/software version' is used, for example:</p> <pre>User-Agent: myproduct/v.6.40.010.006</pre> <p>If not configured, the default string, <AudioCodes product-name>/software version' is used, for example:</p> <pre>User-Agent: Audiocodes-Sip-Gateway-Mediant1000/v.6.40.010.006</pre> <p>The maximum string length is 50 characters.</p> <p>Note: The software version number and preceding forward slash (/) cannot be modified. Therefore, it is recommended not to include a forward slash in the parameter's value (to avoid two forward slashes in the SIP header, which may cause problems).</p>

Parameter	Description
Web/EMS: SDP Session Owner [SIPSDPSessionOwner]	Defines the value of the Owner line ('o' field) in outgoing SDP messages. The valid range is a string of up to 39 characters. The default value is 'AudiocodesGW'. For example: <pre data-bbox="582 427 1390 488">o=AudiocodesGW 1145023829 1145023705 IN IP4 10.33.4.126</pre>
[EnableSDPVersionNegotiation]	Enables the device to ignore new SDP re-offers (from the media negotiation perspective) in certain scenarios (such as session expires). According to RFC 3264, once an SDP session is established, a new SDP offer is considered a new offer only when the SDP origin value is incremented. In scenarios such as session expires, SDP negotiation is irrelevant and thus, the origin field is not changed. 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. <ul style="list-style-type: none"> ▪ [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 Subject header value in outgoing INVITE messages. If not specified, the Subject header isn't included (default). The maximum length is up to 50 characters.
Web: Multiple Packetization Time Format EMS: Multi Ptime Format [MultiPtimeFormat]	Determines whether the 'mptime' attribute is included in the outgoing SDP. <ul style="list-style-type: none"> ▪ [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.
EMS: Enable P Time [EnablePtime]	Determines whether the 'ptime' attribute is included in the SDP. <ul style="list-style-type: none"> ▪ [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, To, and From tags) or change them in the new initiated INVITE. <ul style="list-style-type: none"> ▪ [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. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable

Parameter	Description
Web/EMS: Retry-After Time [RetryAfterTime]	Defines the time (in seconds) used in the Retry-After header when a 503 (Service Unavailable) response is generated by the device. The time range is 0 to 3,600. The default value is 0.
Web/EMS: Fake Retry After [sec] [FakeRetryAfter]	<p>Determines whether the device, upon receipt of a SIP 503 response without a Retry-After header, behaves as if the 503 response included a Retry-After header and with the period (in seconds) specified by this parameter.</p> <ul style="list-style-type: none"> ▪ [0] Disable ▪ Any positive value (in seconds) for defining the period <p>When enabled, this feature allows the device to operate with Proxy servers that do not include the Retry-After SIP header in SIP 503 (Service Unavailable) responses to indicate an unavailable service. The Retry-After header is used with the 503 (Service Unavailable) response to indicate how long the service is expected to be unavailable to the requesting SIP client. The device maintains a list of available proxies, by using the Keep-Alive mechanism. The device checks the availability of proxies by sending SIP OPTIONS every keep-alive timeout to all proxies.</p> <p>If the device receives a SIP 503 response to an INVITE, it also marks that the proxy is out of service for the defined "Retry-After" period.</p>
Web/EMS: Enable P-Associated-URI Header [EnablePAssociatedURIHeader]	<p>Determines the device usage of the P-Associated-URI header. This header can be received in 200 OK responses to REGISTER requests. When enabled, the first URI in the P-Associated-URI header is used in subsequent requests as the From/P-Asserted-Identity headers value.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable. <p>Note: P-Associated-URIs in registration responses is handled only if the device is registered per endpoint (using the User Information file).</p>
Web/EMS: Source Number Preference [SourceNumberPreference]	<p>Determines from which SIP header the source (calling) number is obtained in incoming INVITE messages.</p> <ul style="list-style-type: none"> ▪ If not configured (i.e., empty string) or if any string other than "From" or "Pai2" is configured, the calling number is obtained from a specific header using the following logic: <ul style="list-style-type: none"> a. P-Preferred-Identity header. b. If the above header is not present, then the first P-Asserted-Identity header is used. c. If the above header is not present, then the Remote-Party-ID header is used. d. If the above header is not present, then the From header is used. ▪ "From" = The calling number is obtained from the From header. ▪ "Pai2" = The calling number is obtained using the following logic: <ul style="list-style-type: none"> a. If a P-Preferred-Identity header is present, the number is obtained from it. b. If no P-Preferred-Identity header is present and two P-Asserted-Identity headers are present, the number is obtained from the second P-Asserted-Identity header. c. If only one P-Asserted-Identity header is present, the calling number is obtained from it. <p>Notes:</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ The "From" and "Pai2" values are not case-sensitive. ▪ Once a URL is selected, all the calling party parameters are set from this header. If P-Asserted-Identity is selected and the Privacy header is set to 'id', the calling number is assumed restricted.
[SelectSourceHeaderForCalledNumber]	<p>Determines the SIP header used for obtaining the called number (destination) for IP-to-Tel calls.</p> <ul style="list-style-type: none"> ▪ [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]	<p>Determines how the device handles the receipt of multiple SIP 18x forking responses for Tel-to-IP calls. The forking 18x response is the response with a different SIP to-tag than the previous 18x response. These responses are typically generated (initiated) by Proxy / Application servers that perform call forking, sending the device's originating INVITE (received from SIP clients) to several destinations, using the same CallID.</p> <ul style="list-style-type: none"> ▪ [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. <p>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.</p>
Web: Forking Timeout [ForkingTimeOut]	<p>Defines the timeout (in seconds) that is started after the first SIP 2xx response has been received for a User Agent when a Proxy server performs call forking (Proxy server forwards the INVITE to multiple SIP User Agents). The device sends a SIP ACK and BYE in response to any additional SIP 2xx received from the Proxy within this timeout. Once this timeout elapses, the device ignores any subsequent SIP 2xx.</p> <p>The number of supported forking calls per channel is 20. In other words, for an INVITE message, the device can receive up to 20 forking responses from the Proxy server.</p> <p>The valid range is 0 to 30. The default is 30.</p>
Web: Tel2IP Call Forking Mode [Tel2IPCallForkingMode]	<p>Enables Tel-to-IP call forking, whereby a Tel call can be routed to multiple IP destinations.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note: Once enabled, routing rules must be assigned Forking Groups</p>

Parameter	Description
	in the Outbound IP Routing table.
Web/EMS: Enable Reason Header [EnableReasonHeader]	Enables the usage of the SIP Reason header. <ul style="list-style-type: none"> [0] Disable [1] Enable (default)
Web/EMS: Gateway Name [SIPGatewayName]	Defines a name for the device (e.g., device123.com'). Notes: <ul style="list-style-type: none"> Ensure that the name defined is the one with which the Proxy is configured to identify the device. 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"). <ul style="list-style-type: none"> [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.) <ul style="list-style-type: none"> [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. <ul style="list-style-type: none"> [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. <ul style="list-style-type: none"> [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". <p>This parameter may be useful, for example, for service providers who identify their SIP Trunking customers by their source phone number or IP address, reflected in the From header of the SIP INVITE. Therefore, even customers blocking their Caller ID can be identified by the service provider. Typically, if the device receives a call with blocked Caller ID from the PSTN side (e.g., Trunk connected to a PBX), it sends an INVITE to the IP with a From header as follows: From: "anonymous" <anonymous@anonymous.invalid>. This is in accordance with RFC 3325. However, when this parameter is set to</p>

Parameter	Description
	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.
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. <ul style="list-style-type: none"> ▪ [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 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 471.) <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable
[HandleReasonHeader]	Determines whether the device uses the value of the incoming SIP Reason header for Release Reason mapping. <ul style="list-style-type: none"> ▪ [0] Disregard Reason header in incoming SIP messages. ▪ [1] 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. <ul style="list-style-type: none"> ▪ [0] = Disregard the 'silencesupp' 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. <p>Note: This parameter is applicable only if the G.711 coder is used.</p>
[EnableRport]	Enables the usage of the 'rport' parameter in the Via header. <ul style="list-style-type: none"> ▪ [0] = Disabled (default). ▪ [1] = Enabled. <p>The device adds an 'rport' parameter to the Via header of each outgoing SIP message. The first Proxy that receives this message sets the 'rport' value of the response to the actual port from where the request was received. This method is used, for example, to enable the device to identify its port mapping outside a NAT.</p> <p>If the Via header doesn't include the 'rport' parameter, the destination port of the response is obtained from the host part of the Via header. If the Via header includes the 'rport' parameter without a port value, the destination port of the response is the source port of the incoming request.</p> <p>If the Via header includes 'rport' with a port value (e.g., rport=1001), the destination port of the response is the port indicated in the 'rport' parameter.</p>
Web: Enable X-Channel Header EMS: X Channel Header [XChannelHeader]	Determines whether the SIP X-Channel header is added to SIP messages for providing information on the physical Trunk/B-channel on which the call is received or placed. <ul style="list-style-type: none"> ▪ [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 Trunk number, B-channel,

Parameter	Description
	<p>and the device's IP address. For example, 'x-channel: DS/DS1-5/8;IP=192.168.13.1', where:</p> <ul style="list-style-type: none"> ✓ 'DS/DS-1' is a constant string ✓ '5' is the Trunk number ✓ '8' is the B-channel ✓ 'IP=192.168.13.1' is the device's IP address
<p>Web/EMS: Progress Indicator to IP [ProgressIndicator2IP]</p>	<p>For Analog (FXS/FXO) interfaces:</p> <ul style="list-style-type: none"> ▪ [-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). <p>For Digital interfaces:</p> <ul style="list-style-type: none"> ▪ [-1] Not Configured = for ISDN spans, the progress indicator (PI) that is received in ISDN Proceeding, Progress, and Alerting messages is used as described in the options below. (default) ▪ [0] No PI = For IP-to-Tel calls, the device sends 180 Ringing SIP response to IP after receiving ISDN Alerting or (for CAS) after placing a call to PBX/PSTN. ▪ [1] PI =1, [8] PI =8: For IP-to-Tel calls, if the parameter EnableEarlyMedia is set to 1, the device sends 180 Ringing with SDP in response to an ISDN Alerting or it sends a 183 Session Progress message with SDP in response to only the first received ISDN Proceeding or Progress message after a call is placed to PBX/PSTN over the trunk. <p>Note: This parameter can also be configured per IP Profile (using the IPProfile parameter) and Tel Profile (using the TelProfile parameter).</p>
<p>[EnableRekeyAfter181]</p>	<p>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").</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable <p>Note: This parameter is applicable only if SRTP is used.</p>
<p>[NumberOfActiveDialogs]</p>	<p>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 20. The default value is 20.</p>
<p>[TransparentCoderOnData Call]</p>	<ul style="list-style-type: none"> ▪ [0] = Only use coders from the coder list (default). ▪ [1] = Use Transparent coder for data calls (according to RFC 4040). <p>The Transparent' coder can be used on data calls. When the device receives a Setup message from the ISDN with 'TransferCapabilities = data', it can initiate a call using the coder 'Transparent' (even if the coder is not included in the coder list). The initiated INVITE includes the following SDP attribute:</p>

Parameter	Description
	<p>a=rtpmap:97 CLEARMODE/8000</p> <p>The default payload type is set according to the CodersGroup parameter. If the Transparent coder is not defined, the default value is set to 56. The payload type is negotiated with the remote side, i.e., the selected payload type is according to the remote side selection. The receiving device must include the 'Transparent' coder in its coder list.</p>
Web: Enable IP2IP Application [EnableIP2IPApplication]	Enables the IP-to-IP Call Routing application. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note: For this parameter to take effect, a device reset is required.</p>
[IP2IPTranscodingMode]	Defines the voice transcoding mode (media negotiation) between two user agents for the IP-to-IP application. <ul style="list-style-type: none"> ▪ [0] Only if Required = Do not force transcoding. Many of the media settings (such as gain control) are not implemented on the voice stream. The device passes packets RTP to RTP packets without any processing. ▪ [1] Force = Force transcoding on the outgoing IP leg. The device interworks the media by implementing DSP transcoding. (default)
Web: Enable RFC 4117 Transcoding [EnableRFC4117Transcoding]	Enables transcoding of calls according to RFC 4117. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ For more information on transcoding, see Transcoding using Third-Party Call Control on page 461.
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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 analog interfaces: For information on mapping PSTN release causes to SIP responses, see Mapping PSTN Release Cause to SIP Response on page 280. ▪ When the Trunk is disconnected or is not synchronized, the internal cause is 27. This cause is mapped, by default, to SIP 502. ▪ For mapping SIP-to-Q.931 and Q.931-to-SIP release causes, see Configuring Release Cause Mapping on page 265. ▪ For a list of SIP responses-Q.931 release cause mapping, see 'Release Reason Mapping' on page 240.
Web: Enable Microsoft Extension [EnableMicrosoftExt]	Enables the modification of the called and calling number for numbers received with Microsoft's proprietary "ext=xxx" parameter in the SIP INVITE URI user part. Microsoft Office Communications Server sometimes uses this proprietary parameter to indicate the extension number of the called or calling party.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>For example, if a calling party makes a call to telephone number 622125519100 Ext. 104, the device receives the SIP INVITE (from Microsoft's application) with the URI user part as INVITE sip:622125519100;ext=104@10.1.1.10 (or INVITE tel:622125519100;ext=104). If the parameter EnableMicrosofExt is enabled, the device modifies the called number by adding an "e" as the prefix, removing the "ext=" parameter, and adding the extension number as the suffix (e.g., e622125519100104). Once modified, the device can then manipulate the number further, using the Number Manipulation tables to leave only the last 3 digits (for example) for sending to a PBX.</p>
EMS: Use SIP URI For Diversion Header [UseSIPURIForDiversionHeader]	<p>Defines the URI format in the SIP Diversion header.</p> <ul style="list-style-type: none"> ▪ [0] = 'tel:' (default) ▪ [1] = 'sip:'
[TimeoutBetween100And18x]	<p>Defines the timeout (in msec) between receiving a 100 Trying response and a subsequent 18x response. If a 18x response is not received within this timeout period, the call is disconnected. The valid range is 0 to 180,000 (i.e., 3 minutes). The default value is 32000 (i.e., 32 sec).</p>
[EnableImmediateTrying]	<p>Determines if and when the device sends a 100 Trying in response to an incoming INVITE request.</p> <ul style="list-style-type: none"> ▪ [0] = 100 Trying response is sent upon receipt of a Proceeding message from the PSTN. ▪ [1] = 100 Trying response is sent immediately upon receipt of INVITE request (default).
[TransparentCoderPresentation]	<p>Determines the format of the Transparent coder representation in the SDP.</p> <ul style="list-style-type: none"> ▪ [0] = clearmode (default) ▪ [1] = X-CCD
[IgnoreRemoteSDPMKI]	<p>Determines whether the device ignores the Master Key Identifier (MKI) if present in the SDP received from the remote side.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
[TrunkStatusReportingMode]	<p>Determines whether the device responds to SIP OPTIONS if all the trunks pertaining to Trunk Group #1 are down or busy.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable = If all the trunks pertaining to Trunk Group #1 are down or busy, the device does not respond to received SIP OPTIONS.
Web: Comfort Noise Generation Negotiation EMS: Comfort Noise Generation [ComfortNoiseNegotiation]	<p>Enables negotiation and usage of Comfort Noise (CN).</p> <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default) <p>The use of CN is indicated by including a payload type for CN on the media description line of the SDP. The device can use CN with a codec whose RTP time stamp clock rate is 8,000 Hz (G.711/G.726). The static payload type 13 is used. The use of CN is negotiated between sides. Therefore, if the remote side doesn't support CN, it is</p>

Parameter	Description
	<p>not used. Regardless of the device's settings, it always attempts to adapt to the remote SIP UA's request for CNG, as described below.</p> <p>To determine CNG support, the device uses the ComfortNoiseNegotiation parameter and the codec's SCE (silence suppression setting) using the CodersGroup parameter.</p> <p>If the ComfortNoiseNegotiation parameter is enabled, then the following occurs:</p> <ul style="list-style-type: none"> ▪ 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. <p>If the ComfortNoiseNegotiation parameter is disabled, then the device does not send "CN" in the SDP. However, if the codec's SCE is enabled, then CNG occurs.</p>
Web/EMS: First Call Ringback Tone ID [FirstCallIRBTId]	<p>Defines the index of the first Ringback Tone in the CPT file. This option enables an Application server to request the device to play a distinctive Ringback tone to the calling party according to the destination of the call. The tone is played according to the Alert-Info header received in the 180 Ringing SIP response (the value of the Alert-Info header is added to the value of this parameter). The valid range is -1 to 1,000. The default value is -1 (i.e., play standard Ringback tone).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ It is assumed that all Ringback tones are defined in sequence in the CPT file. ▪ In case of an MLPP call, the device uses the value of 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]	<p>For Analog interfaces: Defines the time interval from when the user hangs up the phone until the call is disconnected (FXS). This allows the user to hang up and then pick up the phone (before this timeout) to continue the call conversation. Thus, it's also referred to as regret time.</p> <p>For Digital interfaces: Defines the time period the device waits for an MFC R2 Resume (Reanswer) signal once a Suspend (Clear back) signal is received from the PBX. If this timer expires, the call is released. Note that this is applicable only to the MFC-R2 CAS Brazil variant.</p> <p>The valid range is 0 to 255 (in seconds). The default value is 0.</p>
Web: Enable Reanswering Info [EnableReansweringINFO]	<p>Enables the device to send a SIP INFO message with the On-Hook/Off-Hook parameter when the FXS phone goes on-hook during an ongoing call and then off-hook again, within the user-defined regret timeout (configured by the parameter RegretTime). Therefore, the device notifies the far-end that the call has been re-answered.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>This parameter is typically implemented for incoming IP-to-Tel collect calls to the FXS port. If the FXS user does not wish to accept the collect call, the user disconnects the call by on-hooking the phone.</p>

Parameter	Description
	<p>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).</p> <p>The INFO message format is as follows:</p> <pre>INFO sip:12345@10.50.228.164:5082 SIP/2.0 Via: SIP/2.0/UDP 127.0.0.1;branch=z9hG4bK_05_905924040-90579 From: <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</pre> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only if the parameter RegretTime is configured. ▪ This parameter is applicable only to FXS interfaces.
<p>Web: PSTN Alert Timeout EMS: Trunk PSTN Alert Timeout [PSTNAlertTimeout]</p>	<p>For digital interfaces: Defines the Alert Timeout (in seconds) for calls sent to the PSTN. This timer is used between the time a Setup message is sent to the Tel side (IP-to-Tel call establishment) and a Connect message is received. If an Alerting message is received, the timer is restarted. If the timer expires before the call is answered, the device disconnects the call and sends a SIP 408 request timeout response to the SIP party that initiated the call.</p> <p>For analog interfaces: Defines the Alert Timeout (in seconds) for calls to the Tel side. This timer is used between the time a ring is generated (FXS) or a line is seized (FXO), until the call is connected. For example: If the FXS device receives an INVITE, it generates a ring to the phone and sends a SIP 180 Ringing response to the IP. If the phone is not answered within the time interval set by this parameter, the device cancels the call by sending a SIP 408 response.</p> <p>The valid value range is 1 to 600 (in seconds). The default is 180.</p> <p>Note: If per trunk configuration (using TrunkPSTNAlertTimeout) is set to other than default, the PSTNAlertTimeout parameter value is overridden.</p>
<p>Web: RTP Only Mode [RTPOnlyMode]</p>	<p>Enables the device to send and receive RTP packets to and from remote endpoints without the need to establish a SIP session. The remote IP address is determined according to the Outbound IP Routing table (Prefix parameter). The port is the same port as the local RTP port (configured by the BaseUDPPort parameter and the channel on which the call is received).</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Transmit & Receive = Send and receive RTP packets ▪ [2] Transmit Only= Send RTP packets only

Parameter	Description
	<ul style="list-style-type: none"> ▪ [3] Receive Only= Receive RTP packets only <p>Notes:</p> <ul style="list-style-type: none"> ▪ To activate the RTP Only feature without using ISDN / CAS signaling, you must do the following: <ul style="list-style-type: none"> ✓ Configure E1/T1 Transparent protocol type (set the ProtoType parameter to 5 or 6). ✓ Enable the TDM-over-IP feature (set the EnableTDMoverIP parameter to 1). ▪ 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.
[RTPOnlyModeForTrunk_ID]	Enables the RTP Only feature per trunk, where ID depicts the trunk number (0 is the first trunk). For more information, see the RTPOnlyMode parameter. <p>Note: For using the global parameter (i.e., setting the RTP Only feature for all trunks), set this parameter to -1 (default).</p>
Web/EMS: SIT Q850 Cause [SITQ850Cause]	Defines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when a Special Information Tone (SIT) is detected on an IP-to-Tel call. The valid range is 0 to 127. The default value is 34. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For mapping specific SIT tones, you can use the SITQ850CauseForNC, SITQ850CauseForIC, SITQ850CauseForVC, and SITQ850CauseForRO parameters.
Web/EMS: SIT Q850 Cause For NC [SITQ850CauseForNC]	Defines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-NC (No Circuit Found Special Information Tone) is detected from the PSTN for IP-to-Tel calls. The valid range is 0 to 127. The default value is 34. <p>Note: When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
Web/EMS: SIT Q850 Cause For IC [SITQ850CauseForIC]	Defines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-IC (Operator Intercept Special Information Tone) is detected from the PSTN for IP-to-Tel calls. The valid range is 0 to 127. The default value is -1 (not configured). <p>Note: When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
Web/EMS: SIT Q850 Cause For VC [SITQ850CauseForVC]	Defines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-VC (Vacant Circuit - non-registered number Special Information Tone) is detected from the PSTN for IP-to-Tel calls. The valid range is 0 to 127. The default value is -1 (not configured). <p>Note: When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
Web/EMS: SIT Q850 Cause For RO [SITQ850CauseForRO]	Defines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when SIT-RO (Reorder - System Busy Special Information Tone) is detected from the PSTN for IP-to-

Parameter	Description
	<p>Tel calls. The valid range is 0 to 127. The default value is -1 (not configured). Note: When not configured (i.e., default), the SITQ850Cause parameter is used.</p>
[GWInboundManipulationSet]	<p>Selects the Manipulation Set ID for manipulating all inbound INVITE messages. The Manipulation Set is defined using the MessageManipulations parameter. By default, no manipulation is done (i.e. Manipulation Set ID is set to -1).</p>
[GWOutboundManipulationSet]	<p>Selects the Manipulation Set ID for manipulating all outbound INVITE messages. The Manipulation Set is defined using the MessageManipulations parameter. By default, no manipulation is done (i.e. Manipulation Set ID is set to -1). Note: This parameter is used only if the Outbound Message Manipulation Set parameter of the destination IP Group is not set.</p>
Out-of-Service (Busy Out) Parameters	
<p>Web/EMS: Enable Busy Out [EnableBusyOut]</p>	<p>Enables the Busy Out feature.</p> <ul style="list-style-type: none"> ▪ [0] Disable = 'Busy out' feature is not used (default). ▪ [1] Enable = 'Busy out' feature is enabled. <p>When Busy Out is enabled and certain scenarios exist, the device performs the following: For analog interfaces: A reorder tone (configured by the parameter FXSOOSBehavior) is played when the phone is off-hooked. For digital interface: All E1/T1 trunks are automatically taken out of service by taking down the D-Channel or by sending a Service Out message for T1 PRI trunks supporting these messages (NI-2, 4/5-ESS, DMS-100, and Meridian).</p> <p>These behaviors are performed upon one of the following scenarios:</p> <ul style="list-style-type: none"> ▪ 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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For Analog interfaces: The FXSOOSBehavior parameter determines the behavior of the FXS endpoints when a Busy Out or Graceful Lock occurs. ▪ For Analog interfaces: FXO endpoints during Busy Out and Lock are inactive. ▪ For Analog interfaces: See the LifeLineType parameter for complementary optional behavior. ▪ For Digital interfaces: The Busy Out behavior varies between different protocol types. ▪ For Digital interfaces: The Busy-Out condition can also be applied to a specific Trunk Group. If there is no connectivity to the Serving

Parameter	Description
	<p>IP Group of a specific Trunk Group (defined in the Trunk Group Settings table), all the physical trunks pertaining to that Trunk Group are set to the Busy-Out condition. Each trunk uses the proper Out-Of-Service method according to the selected ISDN/CAS variant.</p> <ul style="list-style-type: none"> For Digital interfaces: You can use the parameter DigitalOOSBehavior to select the method for setting digital trunks to Out-Of-Service.
Web: Out-Of-Service Behavior EMS:FXS OOS Behavior [FXSOOSBehavior]	<p>Determines the behavior of undefined FXS endpoints and all FXS endpoints when a Busy Out condition exists.</p> <ul style="list-style-type: none"> [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. <p>Note: This parameter is applicable only to FXS interfaces.</p>
Retransmission Parameters	
Web: SIP T1 Retransmission Timer [msec] EMS: T1 RTX [SipT1Rtx]	<p>Defines the time interval (in msec) between the first transmission of a SIP message and the first retransmission of the same message. The default is 500.</p> <p>Note: The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx. For INVITE requests, it is multiplied by two for each new retransmitted message. For all other SIP messages, it is multiplied by two until SipT2Rtx. For example, assuming SipT1Rtx = 500 and SipT2Rtx = 4000:</p> <ul style="list-style-type: none"> The first retransmission is sent after 500 msec. The second retransmission is sent after 1000 (2*500) msec. The third retransmission is sent after 2000 (2*1000) msec. The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec.
Web: SIP T2 Retransmission Timer [msec] EMS: T2 RTX [SipT2Rtx]	<p>Defines the maximum interval (in msec) between retransmissions of SIP messages (except for INVITE requests). The default is 4000.</p> <p>Note: The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.</p>
Web: SIP Maximum RTX EMS: Max RTX [SIPMaxRtx]	<p>Defines the maximum number of UDP transmissions (first transmission plus retransmissions) of SIP messages. The range is 1 to 30. The default value is 7.</p>

Parameter	Description
Web: Number of RTX Before Hot-Swap EMS: Proxy Hot Swap Rtx [HotSwapRtx]	Defines the number of retransmitted INVITE/REGISTER messages before the call is routed (hot swap) to another Proxy/Registrar. The valid range is 1 to 30. The default value is 3. Note: This parameter is also used for alternative routing using the Outbound IP Routing Table'. 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.
SIP Message Manipulations Table	
Web: Message Manipulations EMS: Message Manipulations CLI: configure voip > sbc manipulations message-manipulations [MessageManipulations]	This parameter table defines manipulation rules for SIP header messages. The format of this parameter is as follows: <pre>[MessageManipulations] FORMAT MessageManipulations_Index = MessageManipulations_ManSetID, MessageManipulations_MessageType, MessageManipulations_Condition, MessageManipulations_ActionSubject, MessageManipulations_ActionType, MessageManipulations_ActionValue, MessageManipulations_RowRole; [MessageManipulations]</pre> Where: <ul style="list-style-type: none"> ▪ ManSetID = Defines a Manipulation Set ID for the rule. You can define the same Manipulation Set ID for multiple rules and thereby, create a group of rules that you can assign to an IP entity. The Manipulation Set IDs are later used to assign the manipulation rules to an IP Group ▪ MessageType = Defines the SIP message type (in string format) that you want to manipulate (e.g., Invite.Request). ▪ Condition = Defines the condition that must exist for the rule to apply (e.g., header.from.url.user==100). ▪ ActionSubject = Defines the SIP header upon which the manipulation is performed. ▪ ActionType = Defines the type of manipulation: <ul style="list-style-type: none"> ✓ [0] (default) = adds new header/param/body (header or parameter elements). ✓ [1] = removes header/param/body (header or parameter elements). ✓ [2] = sets element to the new value (all element types). ✓ [3] = adds value at the beginning of the string (string element only). ✓ [4] = adds value at the end of the string (string element only). ✓ [5] = removes value from the end of the string (string element only). ✓ [6] = removes value from the beginning of the string (string element only). ▪ ActionValue = Defines a value (string) that you want to use in the manipulation (e.g., header.from.url.user). ▪ RowRole = Determines which condition must be used for the rule of this table row.

Parameter	Description
	<ul style="list-style-type: none"> ✓ [0] Use Current Condition = The condition entered in this row must be matched in order to perform the defined action (default). ✓ [1] Use Previous Condition = The condition of the rule configured directly above this row must be used in order to perform the defined action. This option allows you to configure multiple actions for the same condition. <p>For example, the below configuration changes the user part of the SIP From header to 200: MessageManipulations 1 = 0, Invite.Request, , Header.From.Url.User, 2, 200, 0;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table can include up to 200 indices (where 1 is the first index). ▪ For a description of the syntax that can be used for this table, see 'SIP Message Manipulation Syntax' on page 769. ▪ You must enclose a string in a single apostrophe. If you are using multiple strings, then the entire string must also be enclosed in double apostrophe, for example, "<sip:' + header.from.url.user + '@domain.com>". ▪ For a description on configuring ini file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.10 Coders and Profile Parameters

The profile parameters are described in the table below.

Table A-32: Profile Parameters

Parameter	Description
Coders Table / Coder Groups Table	
Web: Coders Table/Coder Group Settings EMS: Coders Group [CodersGroup0] [CodersGroup1] [CodersGroup2] [CodersGroup3] [CodersGroup4]	This <i>parameter</i> table 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, <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> ✓ [0] Disabled (default) ✓ [1] Enabled For example, below are defined two Coder Groups (0 and 1):

Parameter	Description																																																																	
	<pre>[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]</pre> <p>The table below lists the supported coders:</p> <table border="1"> <thead> <tr> <th>Coder Name</th> <th>Packetization Time (msec)</th> <th>Rate (kbps)</th> <th>Payload Type</th> <th>Silence Suppression</th> </tr> </thead> <tbody> <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> <tr> <td>G.711A-law_VBD [g711AlawVbd]</td> <td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td> <td>Always 64</td> <td>Dynamic (0-127)</td> <td>N/A</td> </tr> <tr> <td>G.711U-law_VBD [g711UlawVbd]</td> <td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td> <td>Always 64</td> <td>Dynamic (0-127)</td> <td>N/A</td> </tr> <tr> <td>G.722 [g722]</td> <td>20 (default), 40, 60, 80, 100, 120</td> <td>64 (default)</td> <td>Always 9</td> <td>N/A</td> </tr> <tr> <td>G.723.1 [g7231]</td> <td>30 (default), 60, 90, 120</td> <td>5.3 [0] (default), 6.3 [1]</td> <td>Always 4</td> <td>Disable [0] Enable [1]</td> </tr> <tr> <td>G.726 [g726]</td> <td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td> <td>16 [0], 24 [1], 32 [2] (default), 40 [3]</td> <td>Dynamic (0-127) Default is 23</td> <td>Disable [0] Enable [1]</td> </tr> <tr> <td>G.727 ADPCM</td> <td>10, 20 (default), 30, 40, 50, 60, 80, 100, 120</td> <td>16, 24, 32, 40</td> <td>Dynamic (0-127)</td> <td>Disable [0] Enable [1]</td> </tr> <tr> <td>G.729 [g729]</td> <td>10, 20 (default), 30, 40, 50, 60, 80, 100</td> <td>Always 8</td> <td>Always 18</td> <td>Disable [0] Enable [1] Enable w/o Adaptations [2]</td> </tr> <tr> <td>GSM-FR [gsmFullRate]</td> <td>20 (default), 40, 60, 80</td> <td>Always 13</td> <td>Always 3</td> <td>Disable [0] Enable [1]</td> </tr> <tr> <td>GSM-EFR [gsmEnhancedFullRate]</td> <td>0, 20 (default), 30, 40, 50, 60, 80, 100</td> <td>12.2</td> <td>Dynamic (0-127)</td> <td>Disable [0] Enable [1]</td> </tr> <tr> <td>MS-GSM [gsmMS]</td> <td>40 (default)</td> <td>Always 13</td> <td>Always 3</td> <td>Disable [0] Enable [1]</td> </tr> </tbody> </table>	Coder Name	Packetization Time (msec)	Rate (kbps)	Payload Type	Silence Suppression	G.711 A-law [g711Alaw64k]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Always 8	Disable [0] Enable [1]	G.711 U-law [g711Ulaw64k]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Always 0	Disable [0] Enable [1]	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	G.722 [g722]	20 (default), 40, 60, 80, 100, 120	64 (default)	Always 9	N/A	G.723.1 [g7231]	30 (default), 60, 90, 120	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] , 24 [1] , 32 [2] (default), 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]	GSM-FR [gsmFullRate]	20 (default), 40, 60, 80	Always 13	Always 3	Disable [0] Enable [1]	GSM-EFR [gsmEnhancedFullRate]	0, 20 (default), 30, 40, 50, 60, 80, 100	12.2	Dynamic (0-127)	Disable [0] Enable [1]	MS-GSM [gsmMS]	40 (default)	Always 13	Always 3	Disable [0] Enable [1]
Coder Name	Packetization Time (msec)	Rate (kbps)	Payload Type	Silence Suppression																																																														
G.711 A-law [g711Alaw64k]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Always 8	Disable [0] Enable [1]																																																														
G.711 U-law [g711Ulaw64k]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	Always 64	Always 0	Disable [0] Enable [1]																																																														
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																																																														
G.722 [g722]	20 (default), 40, 60, 80, 100, 120	64 (default)	Always 9	N/A																																																														
G.723.1 [g7231]	30 (default), 60, 90, 120	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] , 24 [1] , 32 [2] (default), 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]																																																														
GSM-FR [gsmFullRate]	20 (default), 40, 60, 80	Always 13	Always 3	Disable [0] Enable [1]																																																														
GSM-EFR [gsmEnhancedFullRate]	0, 20 (default), 30, 40, 50, 60, 80, 100	12.2	Dynamic (0-127)	Disable [0] Enable [1]																																																														
MS-GSM [gsmMS]	40 (default)	Always 13	Always 3	Disable [0] Enable [1]																																																														

Parameter	Description				
AMR [Amr]	20 (default)	4.75 [0], 5.15 [1], 5.90 [2], 6.70 [3], 7.40 [4], 7.95 [5], 10.2 [6], 12.2 [7] (default)	Dynamic (0-127)	Disable [0] Enable [1]	
QCELP [QCELP]	20 (default), 40, 60, 80, 100, 120	Always 13	Always 12	Disable [0] Enable [1]	
EVRC [EvrC]	20 (default), 40, 60, 80, 100	Variable [0] (default), 1/8 [1], 1/2 [3], Full [4]	Dynamic (0-127)	Disable [0] Enable [1]	
iLBC [iLBC]	20 (default), 40, 60, 80, 100, 120	15 (default)	Dynamic (0-127)	Disable [0] Enable [1]	
	30 (default), 60, 90, 120	13			
Transparent [Transparent]	10, 20 (default), 40, 60, 80, 100, 120	Always 64	Dynamic (0-127)	Disable [0] Enable [1]	
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.
- Both GSM-FR and MS-GSM coders use Payload Type 3. When using SDP, it isn't possible to differentiate between the two. Therefore, it is recommended not to select both coders simultaneously.
- 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 information on V.152 (and implementation of T.38 and VBD coders), see 'V.152 Support' on page 150.
- For a description of using *ini* file table parameters, see 'Configuring ini File Table Parameters' on page 84.

Parameter	Description															
IP Profile Table																
Web: IP Profile Settings EMS: Protocol Definition > IP Profile [IPProfile]	<p>This <i>parameter</i> table configures the IP Profile table. Each IP Profile ID includes a set of parameters (which are typically configured separately using their individual "global" parameters). You can later assign these IP Profiles to outbound IP routing rules (Prefix parameter), inbound IP routing rules (PSTNPrefix parameter), and IP Groups (IPGroup parameter).</p> <p>The format of this parameter is as follows: [IPProfile] FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference, IpProfile_CodersGroupID, IpProfile_IsFaxUsed, IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor, IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE, IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort, IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP, IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP, IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber, IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume, IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID, IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode, IpProfile_SBCAllowedCodersGroupID, IpProfile_SBCAllowedCodersMode, IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior, IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode, IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID, IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode; [IPProfile]</p> <p>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;</p> <p>Notes:</p> <ul style="list-style-type: none"> 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 border="1"> <thead> <tr> <th>IPProfile Field</th> <th>Web Name</th> <th>Global Parameter</th> </tr> </thead> <tbody> <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> <tr> <td>IpProfile_CodersGroupID</td> <td>Coder Group</td> <td>CodersGroup</td> </tr> </tbody> </table>	IPProfile Field	Web Name	Global Parameter	IpProfile_Index	Profile ID	-	IpProfile_ProfileName	Profile Name	-	IpProfile_IpPreference	Profile Preference	-	IpProfile_CodersGroupID	Coder Group	CodersGroup
IPProfile Field	Web Name	Global Parameter														
IpProfile_Index	Profile ID	-														
IpProfile_ProfileName	Profile Name	-														
IpProfile_IpPreference	Profile Preference	-														
IpProfile_CodersGroupID	Coder Group	CodersGroup														

Parameter	Description		
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 Canceller	EnableEchoCanceller	
IpProfile_CopyDest2RedirectNumber	Copy Destination Number to Redirect Number	CopyDest2RedirectNumber	
IpProfile_MediaSecurityBehaviour	Media Security Behavior	MediaSecurityBehaviour	
IpProfile_CallLimit	Number of Calls Limit	-	
IpProfile_DisconnectOnBrokenConnection	Disconnect on Broken Connection	DisconnectOnBrokenConnection	
IpProfile_FirstTxDTMfOption	First Tx DTMF Option	TxDTMFOption	
IpProfile_SecondTxDTmfOption	Second Tx DTMF Option	TxDTMFOption	

Parameter	Description		
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	SBCExtensionCodersGroupID	
IpProfile_MediaIPVersionPreference	Media IP Version Preference	MediaIPVersionPreference	
IpProfile_TranscodingMode	Transcoding Mode	TranscodingMode	
IpProfile_SBCAllowedCodersGroupID	Allowed Coders Group ID	-	
IpProfile_SBCAllowedCodersMode	Allowed Coders Mode	AllowedCodersGroup0	
IpProfile_SBCMediaSecurityBehaviour	-	SBCMediaSecurityBehaviour	
IpProfile_SBCRFC2833Behavior	-	-	
IpProfile_SBCAlternativeDTMFMethod	-	-	
IpProfile_SBCAssertIdentity	-	SBCAssertIdentity	
IpProfile_EnableQSIGTunneling	-	EnableQSIGTunneling	
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	
IpProfile_SBCDiversionsMode	Diversion Mode	-	
IpProfile_SBCHistoryInfoMode	History Info Mode	-	

Parameter	Description
	<ul style="list-style-type: none"> ▪ The parameter <code>IpPreference</code> 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 <code>CallLimit</code> 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. ▪ <code>RxDtmfOption</code> 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. ▪ <code>FirstTxdtmfOption</code> and <code>SecondTxdtmfOption</code> configures the transmit DTMF negotiation method: [-1] not configured, use the global parameter; for the remaining options, see the global parameter. ▪ The <code>VxxTransportType</code> parameter configures the modem transport type per IP Profile for the following parameters: <code>V21ModemTransportType</code>, <code>V22ModemTransportType</code>, <code>V23ModemTransportType</code>, <code>V32ModemTransportType</code>, and <code>V34ModemTransportType</code>. ▪ IP Profiles can also be used when operating with a Proxy server (set the parameter <code>AlwaysUseRouteTable</code> to 1). ▪ The following parameters are not applicable: <code>IsDTMFUsed</code> (deprecated), <code>SBCExtensionCodersGroupID</code>, <code>TranscodingMode</code>, <code>SBCAllowedCodersGroupID</code>, <code>SBCAllowedCodersMode</code>, <code>SBCMediaSecurityBehaviour</code>, <code>SBCRFC2833Behavior</code>, <code>SBCAlternativeDTMFMethod</code>, <code>SBCAssertIdentity</code>, <code>SBCDiversionMode</code>, <code>SBCHistoryInfoMode</code>, <code>MediaIPVersionPreference</code> ▪ For a description of using <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Tel Profile Table	
Web: Tel Profile Settings EMS: Protocol Definition > Telephony Profile [TelProfile]	This <i>parameter</i> table configures the Tel Profile table. Each Tel Profile ID includes a set of parameters (which are typically configured separately using their individual, "global" parameters). You can later assign these Tel Profile IDs to other elements such as in the Trunk Group Table (<code>TrunkGroup</code> 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: <pre>[TelProfile] FORMAT TelProfile_Index = TelProfile_ProfileName, TelProfile_TelPreference, TelProfile_CodersGroupID, TelProfile_IsFaxUsed, TelProfile_JitterBufMinDelay, TelProfile_JitterBufOptFactor, TelProfile_IPDiffServ, TelProfile_SigIPDiffServ, TelProfile_DtmfVolume, TelProfile_InputGain, TelProfile_VoiceVolume, TelProfile_EnableReversePolarity, TelProfile_EnableCurrentDisconnect, TelProfile_EnableDigitDelivery, TelProfile_EnableEC, TelProfile_MWIAAnalog, TelProfile_MWIDisplay, TelProfile_FlashHookPeriod, TelProfile_EnableEarlyMedia, TelProfile_ProgressIndicator2IP, TelProfile_TimeForReorderTone, TelProfile_EnableDIDWink, TelProfile_IsTwoStageDial, TelProfile_DisconnectOnBusyTone,</pre>

Parameter	Description																																																			
	<p>TelProfile_EnableVoiceMailDelay, TelProfile_DialPlanIndex, TelProfile_Enable911PSAP, TelProfile_SwapTelTolpPhoneNumbers, TelProfile_EnableAGC, TelProfile_ECNIpMode; TelProfile_DigitalCutThrough; [TelProfile]</p> <p>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;</p> <p>Notes:</p> <ul style="list-style-type: none"> 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 border="1"> <thead> <tr> <th>TelProfile Field</th> <th>Web Name</th> <th>Global Parameter</th> </tr> </thead> <tbody> <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> <tr> <td>TelProfile_EnableCurrentDisconnect</td> <td>Enable Current Disconnect</td> <td>EnableCurrentDisconnect</td> </tr> <tr> <td>TelProfile_EnableDigitDelivery</td> <td>Enable Digit Delivery</td> <td>EnableDigitDelivery</td> </tr> <tr> <td>TelProfile_EnableEC</td> <td>Echo Canceler</td> <td>EnableEchoCanceller</td> </tr> <tr> <td>TelProfile_MWIAAnalog</td> <td>MWI Analog Lamp</td> <td>MWIAAnalogLamp</td> </tr> </tbody> </table>	TelProfile Field	Web Name	Global Parameter	TelProfile_ProfileName	Profile Name	-	TelProfile_TelPreference	Profile Preference	-	TelProfile_CodersGroupID	Coder Group	CodersGroup0	TelProfile_IsFaxUsed	Fax Signaling Method	IsFaxUsed	TelProfile_JitterBufMinDelay	Dynamic Jitter Buffer Minimum Delay	DJBufMinDelay	TelProfile_JitterBufOptFactor	Dynamic Jitter Buffer Optimization Factor	DJBufOptFactor	TelProfile_IPDiffServ	RTP IP DiffServ	PremiumServiceClassMediaDiffServ	TelProfile_SigIPDiffServ	Signaling DiffServ	PremiumServiceClassControlDiffServ	TelProfile_DtmfVolume	DTMF Volume	DTMFVolume	TelProfile_InputGain	Input Gain	InputGain	TelProfile_VoiceVolume	Voice Volume	VoiceVolume	TelProfile_EnableReversePolarity	Enable Polarity Reversal	EnableReversalPolarity	TelProfile_EnableCurrentDisconnect	Enable Current Disconnect	EnableCurrentDisconnect	TelProfile_EnableDigitDelivery	Enable Digit Delivery	EnableDigitDelivery	TelProfile_EnableEC	Echo Canceler	EnableEchoCanceller	TelProfile_MWIAAnalog	MWI Analog Lamp	MWIAAnalogLamp
TelProfile Field	Web Name	Global Parameter																																																		
TelProfile_ProfileName	Profile Name	-																																																		
TelProfile_TelPreference	Profile Preference	-																																																		
TelProfile_CodersGroupID	Coder Group	CodersGroup0																																																		
TelProfile_IsFaxUsed	Fax Signaling Method	IsFaxUsed																																																		
TelProfile_JitterBufMinDelay	Dynamic Jitter Buffer Minimum Delay	DJBufMinDelay																																																		
TelProfile_JitterBufOptFactor	Dynamic Jitter Buffer Optimization Factor	DJBufOptFactor																																																		
TelProfile_IPDiffServ	RTP IP DiffServ	PremiumServiceClassMediaDiffServ																																																		
TelProfile_SigIPDiffServ	Signaling DiffServ	PremiumServiceClassControlDiffServ																																																		
TelProfile_DtmfVolume	DTMF Volume	DTMFVolume																																																		
TelProfile_InputGain	Input Gain	InputGain																																																		
TelProfile_VoiceVolume	Voice Volume	VoiceVolume																																																		
TelProfile_EnableReversePolarity	Enable Polarity Reversal	EnableReversalPolarity																																																		
TelProfile_EnableCurrentDisconnect	Enable Current Disconnect	EnableCurrentDisconnect																																																		
TelProfile_EnableDigitDelivery	Enable Digit Delivery	EnableDigitDelivery																																																		
TelProfile_EnableEC	Echo Canceler	EnableEchoCanceller																																																		
TelProfile_MWIAAnalog	MWI Analog Lamp	MWIAAnalogLamp																																																		

Parameter	Description		
TelProfile_MWIDisplay	MWI Display		MWIDisplay
TelProfile_FlashHookPeriod	Flash Hook Period		FlashHookPeriod
TelProfile_EnableEarlyMedia	Enable Early Media		EnableEarlyMedia
TelProfile_ProgressIndicator2IP	Progress Indicator to IP		ProgressIndicator2IP
TelProfile_TimeForReorderTone	Time For Reorder Tone		TimeForReorderTone
TelProfile_EnableDIDWink	Enable DID Wink		EnableDIDWink
TelProfile_IsTwoStageDial	Dialing Mode		IsTwoStageDial
TelProfile_DisconnectOnBusyTone	Disconnect Call on Detection of Busy Tone		DisconnectOnBusyTone
TelProfile_EnableVoiceMailDelay	Enable Voice Mail Delay		-
TelProfile_DialPlanIndex	Dial Plan Index		DialPlanIndex
TelProfile_Enable911PSAP	Enable 911 PSAP		Enable911PSAP
TelProfile_SwapTelToIPPhoneNumbers	Swap Tel To IP Phone Numbers		SwapTEI2IPCalled&CallingNumbers
TelProfile_EnableAGC	Enable AGC		EnableAGC
TelProfile_ECNIpMode	EC NLP Mode		ECNLPMode
TelProfile_DigitalCutThrough	-		DigitalCutThrough
<ul style="list-style-type: none"> ▪ The following parameters are applicable only to analog interfaces: EnableReversePolarity, EnableCurrentDisconnect, MWIAnalog, MWIDisplay, EnableDIDWink, IsTwoStageDial, DisconnectOnBusyTone, and Enable911PSAP. ▪ 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 parameters take precedence. ▪ The parameter EnableVoiceMailDelay is applicable only if voice mail is enabled globally (using the VoiceMailInterface parameter). ▪ For a description of using <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84. 			

A.11 Channel Parameters

This subsection describes the device's channel parameters.

A.11.1 Voice Parameters

The voice parameters are described in the table below.

Table A-33: Voice Parameters

Parameter	Description
Web/EMS: Input Gain [InputGain]	<p>Defines the pulse-code modulation (PCM) input gain control (in decibels). This parameter sets the level for the received (Tel/PSTN-to-IP) signal.</p> <p>The valid range is -32 to 31 dB. The default value is 0 dB.</p> <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 217) and per Tel Profile, using the TelProfile parameter (see 'Configuring Tel Profiles' on page 215).</p>
Web: Voice Volume EMS: Volume (dB) [VoiceVolume]	<p>Defines the voice gain control (in decibels). This parameter sets the level for the transmitted (IP-to-Tel/PSTN) signal.</p> <p>The valid range is -32 to 31 dB. The default value is 0 dB.</p> <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 217) and per Tel Profile, using the TelProfile parameter (see 'Configuring Tel Profiles' on page 215).</p>
EMS: Payload Format [VoicePayloadFormat]	<p>Determines the bit ordering of the G.726/G.727 voice payload format.</p> <ul style="list-style-type: none"> ▪ [0] = Little Endian (default) ▪ [1] = Big Endian <p>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).</p>
Web: MF Transport Type [MFTransportType]	Currently, not supported.
Web: Enable Answer Detector [EnableAnswerDetector]	Currently, not supported.
Web: Answer Detector Activity Delay [AnswerDetectorActivityDelay]	<p>Defines the time (in 100-msec resolution) between activating the Answer Detector and the time that the detector actually starts to operate.</p> <p>The valid range is 0 to 1023. The default is 0.</p>
Web: Answer Detector Silence Time [AnswerDetectorSilenceTime]	Currently, not supported.
Web: Answer Detector Redirection [AnswerDetectorRedirection]	Currently, not supported.

Parameter	Description
Web: Answer Detector Sensitivity EMS: Sensitivity [AnswerDetectorSensitivity]	Defines the Answer Detector sensitivity. The range is 0 (most sensitive) to 2 (least sensitive). The default is 0.
Web: Silence Suppression EMS: Silence Compression Mode [EnableSilenceCompression]	Determines the Silence Suppression support. Silence Suppression is a method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. <ul style="list-style-type: none"> ▪ [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). <p>Note: If the selected coder is G.729, the value of the 'annexb' parameter of the fntp attribute in the SDP is determined by the following rules:</p> <ul style="list-style-type: none"> ▪ 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'. <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 217).</p>
Web: Echo Canceller EMS: Echo Canceller Enable [EnableEchoCanceller]	Enables echo cancellation (i.e., echo from voice calls is removed). <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default) <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 217) and per Tel Profile, using the TelProfile parameter (see 'Configuring Tel Profiles' on page 215).</p>
Web: Max Echo Canceller Length [MaxEchoCancellerLength]	Defines the maximum Echo Canceller Length (in msec), which is the maximum echo path delay (tail length) for which the echo canceller is designed to operate: <ul style="list-style-type: none"> ▪ [0] Default = based on various internal device settings to attain maximum channel capacity (default) ▪ [11] 64 msec ▪ [22] 128 msec <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ Using 128 msec may reduce channel capacity. For example: with DSP Template 0 and number of spans 4, the capacity is reduced from 120 to 100. The reduction depends on the combination of "DSP Template" and "Number of Spans". For accurate figures, see DSP Templates on page 815. ▪ When housed with an analog/BRI module, the device (Mediant 1000) can use a max. echo canceller length of 64 msec. ▪ When housed with PRI TRUNKS module, the device (Mediant 1000) can use a max. echo canceller length of 128 msec. ▪ When housed with an MPM module (in Slot #6), no channel reduction occurs (for Mediant 1000). ▪ It is unnecessary to configure the parameter

Parameter	Description
	EchoCancellerLength, as it automatically acquires its value from this parameter.
EMS: Echo Canceller Hybrid Loss [ECHybridLoss]	Defines the four-wire to two-wire worst-case Hybrid loss, the ratio between the signal level sent to the hybrid and the echo level returning from the hybrid. <ul style="list-style-type: none"> [0] = 6 dB (default) [1] = N/A [2] = 0 dB [3] = 3 dB
[ECNLPMode]	Defines the echo cancellation Non-Linear Processing (NLP) mode. <ul style="list-style-type: none"> [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 215).
[EchoCancellerAggressiveNLP]	Enables the Aggressive NLP at the first 0.5 second of the call. <ul style="list-style-type: none"> [0] = Disable [1] = Enable (default). The echo is removed only in the first half of a second of the incoming IP signal. Note: For this parameter to take effect, a device reset is required.
[RTPSIDCoeffNum]	Defines 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].

A.11.2 Coder Parameters

The coder parameters are described in the table below.

Table A-34: Coder Parameters

Parameter	Description
[EnableEVRCVAD]	Enables the EVRC voice activity detector. <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable Note: Supported for EVRC and EVRC-B coders.
EMS: VBR Coder DTX Min [EVRCDTXMin]	Defines the minimum gap between two SID frames when using the EVRC voice activity detector. Units are in EVRC frame size (20 msec). The range is 0 to 20000. The default value is 12. Note: Supported for EVRC and EVRC-B coders.
EMS: VBR Coder DTX Max [EVRCDTXMax]	Defines the maximum gap between two SID frames when using the EVRC voice activity detector. Units are in EVRC frame size (20 msec). The range is 0 to 20000. The default value is 32. Note: This parameter is applicable only to EVRC and EVRC-B coders.
EMS: VBR Coder Header Format	Determines the format of the RTP header for VBR coders. <ul style="list-style-type: none"> [0] = Payload only (no header, TOC, or m-factor) - similar to RFC

Parameter	Description
[VBRCoderHeaderFormat]	3558 Header Free format (default). <ul style="list-style-type: none"> ▪ [1] = Supports RFC 2658 - 1 byte for interleaving header (always 0), TOC, no m-factor. ▪ [2] = Payload including TOC only, allow m-factor. ▪ [3] = RFC 3558 Interleave/Bundled format.
EMS: VBR Coder Hangover [VBRCoderHangover]	Defines the required number of silence frames at the beginning of each silence period when using the VBR coder silence suppression. The range is 0 to 255. The default value is 1.
Web: DSP Template Mix Table EMS: VoP Media Provisioning > General Settings	
[DSPTemplates]	This parameter table allows the device to use a combination of two DSP templates and determines the percentage of DSP resources allocated per DSP template. The format of this parameter is as follows: [DspTemplates] FORMAT DspTemplates_Index = DspTemplates_DspTemplateName, DspTemplates_DspResourcesPercentage; [DspTemplates] For example, to load DSP Template 1 to 50% of the DSPs, and DSP Template 2 to the remaining 50%, the table is configured as follows: DspTemplates 0 = 1, 50; DspTemplates 1 = 2, 50; Notes: <ul style="list-style-type: none"> ▪ The DSPVersionTemplateName parameter is ignored when the DSPTemplates parameter is configured. ▪ For a list of supported DSP templates, see DSP Templates on page 815.
Web: DSP Version Template Number EMS: Version Template Number [DSPVersionTemplateName]	Determines the DSP template used by the device. Each DSP template supports specific coders, channel capacity, and features. The default is DSP template 0. You can load different DSP templates to analog and digital modules using the syntax DSPVersionTemplateName=xy where: <ul style="list-style-type: none"> ▪ x = 0 or 1 for DSP templates of analog modules ▪ y = 0 to 5 for DSP templates of digital and MPM modules Notes: <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ For a list of supported DSP templates, see DSP Templates on page 815.

A.11.3 DTMF Parameters

The dual-tone multi-frequency (DTMF) parameters are described in the table below.

Table A-35: DTMF Parameters

Parameter	Description
Web/EMS: DTMF Transport Type [DTMFTransportType]	<p>Determines the DTMF transport type.</p> <ul style="list-style-type: none"> ▪ [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. <p>Note: This parameter is automatically updated if the parameters TxDTMFOption or RxDTMFOption are configured.</p>
Web: DTMF Volume (-31 to 0 dB) EMS: DTMF Volume (dBm) [DTMFVolume]	<p>Defines the DTMF gain control value (in decibels) to the PSTN or analog side. The valid range is -31 to 0 dB. The default value is -11 dB.</p> <p>Note: This parameter can also be configured per Tel Profile, using the TelProfile parameter.</p>
Web: DTMF Generation Twist EMS: DTMF Twist Control [DTMFGenerationTwist]	<p>Defines the range (in decibels) between the high and low frequency components in the DTMF signal. Positive decibel values cause the higher frequency component to be stronger than the lower one. Negative values cause the opposite effect. For any parameter value, both components change so that their average is constant. The valid range is -10 to 10 dB. The default value is 0 dB.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: DTMF Inter Interval (msec) [DTMFInterDigitInterval]	<p>Defines the 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.</p>
EMS: DTMF Length (msec) [DTMFDigitLength]	<p>Defines the time (in msec) for generating DTMF tones to the PSTN side (if TxDTMFOption = 1, 2 or 3). It also configures the duration that is sent in INFO (Cisco) messages. The valid range is 0 to 32767. The default value is 100.</p>
EMS: Rx DTMF Relay Hang Over Time (msec) [RxDTMFHangOverTime]	<p>Defines the Voice Silence time (in msec) after playing DTMF or MF digits to the Tel/PSTN side that arrive as Relay from the IP side. Valid range is 0 to 2,000 msec. The default is 1,000 msec.</p>
EMS: Tx DTMF Relay Hang Over Time (msec) [TxDTMFHangOverTime]	<p>Defines the Voice Silence time (in msec) after detecting the end of DTMF or MF digits at the Tel/PSTN side when the DTMF Transport Type is either Relay or Mute. Valid range is 0 to 2,000 msec. The default is 1,000 msec.</p>
Web/EMS: NTE Max Duration [NTEMaxDuration]	<p>Defines the maximum time for sending Named Telephony Events / NTEs (RFC 4733/2833 DTMF relay) to the IP side, regardless of the DTMF signal duration on the TDM side. The range is -1 to 200,000,000 msec (i.e., 300 msec). The default is -1 (i.e., NTE stops only upon detection of an End event).</p>

A.11.4 RTP, RTCP and T.38 Parameters

The RTP, RTCP and T.38 parameters are described in the table below.

Table A-36: RTP/RTCP and T.38 Parameters

Parameter	Description
Web: Dynamic Jitter Buffer Minimum Delay EMS: Minimal Delay (dB) [DJBufMinDelay]	Defines the minimum delay (in msec) for the Dynamic Jitter Buffer. The valid range is 0 to 150. The default delay is 10. Notes: <ul style="list-style-type: none"> 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 153.
Web: Dynamic Jitter Buffer Optimization Factor EMS: Opt Factor [DJBufOptFactor]	Defines the Dynamic Jitter Buffer frame error/delay optimization factor. The valid range is 0 to 12. The default factor is 10. Notes: <ul style="list-style-type: none"> 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 153.
Web/EMS: Analog Signal Transport Type [AnalogSignalTransportType]	Determines the analog signal transport type. <ul style="list-style-type: none"> [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]	Enables the device to generate RFC 2198 redundant packets. This can be used for packet loss where the missing information (audio) can be reconstructed at the receiver's end from the redundant data that arrives in subsequent packets. This is required, for example, in wireless networks where a high percentage (up to 50%) of packet loss can be experienced. <ul style="list-style-type: none"> [0] 0 = Disable (default) [1] 1 = Enable - previous voice payload packet is added to current packet. Notes: <ul style="list-style-type: none"> When enabled, you can configure the payload type, using the RFC2198PayloadType parameter. The RTP redundancy dynamic payload type can be included in the SDP, by using the EnableRTPRedundancyNegotiation parameter. This parameter can also be configured per IP Profile, using the IPProfile parameter.
Web: Enable RTP Redundancy Negotiation [EnableRTPRedundancyNegotiation]	Enables the device to included the RTP redundancy dynamic payload type in the SDP, according to RFC 2198. <ul style="list-style-type: none"> [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	Description
	<p>parameter RFC2198PayloadType.</p> <pre>a=rtpmap:<PT> RED/8000</pre> <p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> 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.
<p>Web: RFC 2198 Payload Type EMS: Redundancy Payload Type [RFC2198PayloadType]</p>	<p>Defines the RTP redundancy packet payload type according to RFC 2198. The range is 96 to 127. The default is 104.</p> <p>Note: This parameter is applicable only if the parameter RTPRedundancyDepth is set to 1.</p>
<p>Web: Packing Factor EMS: Packetization Factor [RTPPackagingFactor]</p>	<p>N/A. Controlled internally by the device according to the selected coder.</p>
<p>Web/EMS: Basic RTP Packet Interval [BasicRTPPacketInterval]</p>	<p>N/A. Controlled internally by the device according to the selected coder.</p>
<p>Web: RTP Directional Control [RTPDirectionControl]</p>	<p>N/A. Controlled internally by the device according to the selected coder.</p>
<p>Web/EMS: RFC 2833 TX Payload Type [RFC2833TxPayloadType]</p>	<p>Defines the Tx RFC 2833 DTMF relay dynamic payload type. The valid range is 96 to 99, and 106 to 127. The default is 96. The 100, 102 to 105 range is allocated for proprietary usage.</p> <p>Notes:</p> <ul style="list-style-type: none"> 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.
<p>Web/EMS: RFC 2833 RX Payload Type [RFC2833RxPayloadType]</p>	<p>Defines the Rx RFC 2833 DTMF relay dynamic payload type. The valid range is 96 to 99, and 106 to 127. The default is 96. The 100, 102 to 105 range is allocated for proprietary usage.</p> <p>Notes:</p> <ul style="list-style-type: none"> 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.

Parameter	Description
[EnableDetectRemoteMACChange]	<p>Determines whether the device changes the RTP packets according to the MAC address of received RTP packets and according to Gratuitous Address Resolution Protocol (GARP) messages.</p> <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Defines the lower boundary of the UDP port used for RTP, RTCP (RTP port + 1) and T.38 (RTP port + 2). For example, if the Base UDP Port is set to 6000, then one channel may use the ports RTP 6000, RTCP 6001, and T.38 6002, while another channel may use RTP 6010, RTCP 6011, and T.38 6012, and so on. The range of possible UDP ports is 6,000 to 64,000. The default base UDP port is 6000.</p> <p>Once this parameter is configured, the UDP port range (lower to upper boundary) is calculated as follows:</p> <ul style="list-style-type: none"> ▪ BaseUDPport to (BaseUDPport + 255*10) <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 on page 170). ▪ If RTP Base UDP Port is not a factor of 10, the following message is generated: 'invalid local RTP port'. ▪ For more information on the default RTP/RTCP/T.38 port allocation, refer to the <i>Product Reference Manual</i>.
Web: Remote RTP Base UDP Port EMS: Remote Base UDP Port [RemoteBaseUDPPort]	<p>Defines 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.</p> <p>The valid range is the range of possible UDP ports: 6,000 to 64,000.</p> <p>The default value is 0 (i.e., RTP multiplexing is disabled).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.

Parameter	Description
	<ul style="list-style-type: none"> This parameter can also be configured per IP Profile, using the IPProfile parameter. For more information on RTP multiplexing, see RTP Multiplexing (ThroughPacket) on page 157.
EMS: No Op Enable [NoOpEnable]	<p>Enables the transmission of RTP or T.38 No-Op packets.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable <p>This mechanism ensures that the NAT binding remains open during RTP or T.38 silence periods.</p>
EMS: No Op Interval [NoOpInterval]	<p>Defines the time interval in which RTP or T.38 No-Op packets are sent in the case of silence (no RTP/T.38 traffic) when No-Op packet transmission is enabled. The valid range is 20 to 65,000 msec. The default is 10,000.</p> <p>Note: To enable No-Op packet transmission, use the NoOpEnable parameter.</p>
EMS: No Op Payload Type [RTPNoOpPayloadType]	<p>Defines 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.</p> <p>Note: When defining this parameter, ensure that it doesn't cause collision with other payload types.</p>
[RTCPActivationMode]	<p>Disables RTCP traffic when there is no RTP traffic. This feature is useful, for example, to stop RTCP traffic that is typically sent when calls are put on hold (by an INVITE with 'a=inactive' in the SDP).</p> <ul style="list-style-type: none"> [0] Active Always = RTCP is active even during inactive RTP periods, i.e., when the media is in 'recvonly' or 'inactive' mode. (default) [1] Inactive Only If RTP Inactive = No RTCP is sent when RTP is inactive.
<p>RTP Control Protocol Extended Reports (RTCP XR) Parameters (Note: For a detailed description of RTCP XR reports, refer to the Product Reference Manual.)</p>	
Web: Enable RTCP XR EMS: RTCP XR Enable [VQMonEnable]	<p>Enables voice quality monitoring and RTCP Extended Reports (RTCP XR), according to Internet-Draft draft-ietf-sipping-rtcp-summary-13.</p> <ul style="list-style-type: none"> [0] Disable = Disable (default) [1] Enable = Enables <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: Minimum Gap Size EMS: GMin [VQMonGMin]	<p>Defines the voice quality monitoring - minimum gap size (number of frames). The default is 16.</p>
Web/EMS: Burst Threshold [VQMonBurstHR]	<p>Defines the voice quality monitoring - excessive burst alert threshold. if set to -1 (default), no alerts are issued.</p>
Web/EMS: Delay Threshold [VQMonDelayTHR]	<p>Defines the voice quality monitoring - excessive delay alert threshold. if set to -1 (default), no alerts are issued.</p>

Parameter	Description
Web: R-Value Delay Threshold EMS: End of Call Rval Delay Threshold [VQMonEOCRValTHR]	Defines the voice quality monitoring - end of call low quality alert threshold. if set to -1 (default), no alerts are issued.
Web: RTCP XR 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 XR Interval Randomization EMS: Disable Interval Randomization [DisableRTCPRandomize]	Determines whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter RTCPInterval. <ul style="list-style-type: none"> ▪ [0] Disable = Randomize (default) ▪ [1] Enable = No Randomize
EMS: RTCP XR Collection Server Transport Type [RTCPXRESCTransportType]	Determines the transport layer used for outgoing SIP dialogs initiated by the device to the RTCP-XR Collection Server. <ul style="list-style-type: none"> ▪ [-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: RTCP XR Collection Server EMS: Esc IP [RTCPXREscIP]	Defines the IP address of the Event State Compositor (ESC). The device sends RTCP XR reports to this server, using SIP PUBLISH messages. The address can be configured as a numerical IP address or as a domain name.
Web: RTCP XR Report Mode EMS: Report Mode [RTCPXRReportMode]	Determines whether RTCP XR reports are sent to the Event State Compositor (ESC) and defines the interval in which they are sent. <ul style="list-style-type: none"> ▪ [0] Disable = RTCP XR reports are not sent to the ESC (default). ▪ [1] End Call = RTCP XR reports are sent to the ESC at the end of each call. ▪ [2] End Call & Periodic = RTCP XR reports are sent to the ESC at the end of each call and periodically according to the parameter RTCPInterval.

A.12 Gateway and IP-to-IP Parameters

A.12.1 Fax and Modem Parameters

The fax and modem parameters are described in the table below.

Table A-37: Fax and Modem Parameters

Parameter	Description
Web: Fax Transport Mode EMS: Transport Mode [FaxTransportMode]	<p>Determines the fax transport mode used by the device.</p> <ul style="list-style-type: none"> ▪ [0] Disable = transparent mode ▪ [1] T.38 Relay (default) ▪ [2] Bypass ▪ [3] Events Only <p>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).</p>
Web: V.21 Modem Transport Type EMS: V21 Transport [V21ModemTransportType]	<p>Determines the V.21 modem transport type.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (Transparent) - default ▪ [1] Enable Relay = N/A ▪ [2] Enable Bypass. ▪ [3] Events Only = Transparent with Events <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 217).</p>
Web: V.22 Modem Transport Type EMS: V22 Transport [V22ModemTransportType]	<p>Determines the V.22 modem transport type.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (Transparent) ▪ [1] Enable Relay = N/A ▪ [2] Enable Bypass = (default) ▪ [3] Events Only = Transparent with Events <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 217).</p>
Web: V.23 Modem Transport Type EMS: V23 Transport [V23ModemTransportType]	<p>Determines the V.23 modem transport type.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (Transparent) ▪ [1] Enable Relay = N/A ▪ [2] Enable Bypass = (default) ▪ [3] Events Only = Transparent with Events <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 217).</p>
Web: V.32 Modem Transport Type EMS: V32 Transport [V32ModemTransportType]	<p>Determines the V.32 modem transport type.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (Transparent) ▪ [1] Enable Relay = N/A ▪ [2] Enable Bypass = (default) ▪ [3] Events Only = Transparent with Events <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 217).

Parameter	Description
Web: V.34 Modem Transport Type EMS: V34 Transport [V34ModemTransportType]	Determines the V.90/V.34 modem transport type. <ul style="list-style-type: none"> ▪ [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 217).
EMS: Bell Transport Type [BellModemTransportType]	Determines the Bell modem transport method. <ul style="list-style-type: none"> ▪ [0] = Transparent (default) ▪ [2] = Bypass ▪ [3] = Transparent with events
Web/EMS: Fax CNG Mode [FaxCNGMode]	Determines the device's behavior upon detection of a CNG tone. <ul style="list-style-type: none"> ▪ [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/EMS: CNG Detector Mode [CNGDetectorMode]	Determines whether the device detects the fax Calling tone (CNG). <ul style="list-style-type: none"> ▪ [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 217).
Web: Fax Relay Enhanced Redundancy Depth EMS: Enhanced Relay Redundancy Depth [FaxRelayEnhancedRedundancyDepth]	Defines the 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]	Defines the number of times that each fax relay payload is retransmitted to the network. <ul style="list-style-type: none"> ▪ [0] = No redundancy (default). ▪ [1] = One packet redundancy. ▪ [2] = Two packet redundancy. Note: This parameter is applicable only to non-V.21 packets.

Parameter	Description
Web: Fax Relay Max Rate (bps) EMS: Relay Max Rate [FaxRelayMaxRate]	<p>Defines the maximum rate (in bps) at which fax relay messages are transmitted (outgoing calls).</p> <ul style="list-style-type: none"> ▪ [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) <p>Note: 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.</p>
Web: Fax Relay ECM Enable EMS: Relay ECM Enable [FaxRelayECMEnable]	<p>Enables Error Correction Mode (ECM) mode during fax relay.</p> <ul style="list-style-type: none"> ▪ [0] Disable. ▪ [1] Enable (default).
Web: Fax/Modem Bypass Coder Type EMS: Coder Type [FaxModemBypassCoderType]	<p>Determines the coder used by the device when performing fax/modem bypass. Typically, high-bit-rate coders such as G.711 should be used.</p> <ul style="list-style-type: none"> ▪ [0] G.711Alaw= G.711 A-law 64 (default). ▪ [1] G.711Mulaw = G.711 μ-law.
Web: Fax/Modem Bypass Packing Factor EMS: Packetization Period [FaxModemBypassM]	<p>Defines the number (20 msec) of coder payloads used to generate a fax/modem bypass packet. The valid range is 1, 2, or 3 coder payloads. The default value is 1 coder payload.</p>
[FaxModemNTEMode]	<p>Determines whether the device sends RFC 2833 ANS/ANSam events upon detection of fax and/or modem Answer tones (i.e., CED tone).</p> <ul style="list-style-type: none"> ▪ [0] = Disabled (default). ▪ [1] = Enabled. <p>Note: This parameter is applicable only when the fax or modem transport type is set to bypass or Transparent-with-Events.</p>
Web/EMS: Fax Bypass Payload Type [FaxBypassPayloadType]	<p>Defines the fax bypass RTP dynamic payload type. The valid range is 96 to 120. The default value is 102.</p>
EMS: Modem Bypass Payload Type [ModemBypassPayloadType]	<p>Defines the modem bypass dynamic payload type. The range is 0-127. The default value is 103.</p>
EMS: Relay Volume (dBm) [FaxModemRelayVolume]	<p>Defines the fax gain control. The range is -18 to -3, corresponding to -18 dBm to -3 dBm in 1-dB steps. The default is -6 dBm fax gain control.</p>
Web/EMS: Fax Bypass Output Gain [FaxBypassOutputGain]	<p>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).</p>
Web/EMS: Modem Bypass Output Gain [ModemBypassOutputGain]	<p>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).</p>

Parameter	Description
n]	
EMS: Basic Packet Interval [FaxModemBypassBasicRTPPacketInterval]	Defines the basic frame size used during fax/modem bypass sessions. <ul style="list-style-type: none"> ▪ [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) [FaxModemBypassJitterBufferMinDelay]	Defines the Jitter Buffer delay (in milliseconds) during fax and modem bypass session. The range is 0 to 150 msec. The default is 40.
EMS: Enable Inband Network Detection [EnableFaxModemInbandNetworkDetection]	Enables in-band network detection related to fax/modem. <ul style="list-style-type: none"> ▪ [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]	Enables Cisco compatible fax and modem bypass mode. <ul style="list-style-type: none"> ▪ [0] = NSE disabled (default) ▪ [1] = NSE enabled In NSE bypass mode, the device starts using G.711 A-Law (default) or G.711 μ -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: <ul style="list-style-type: none"> ▪ 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: 'a=rtptime:100 X-NSE/8000'. ▪ To use this feature: <ul style="list-style-type: none"> ✓ 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 217).
EMS: NSE Payload Type [NSEPayloadType]	Defines the 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.

Parameter	Description
EMS: T38 Use RTP Port [T38UseRTPPort]	Defines the port (with relation to RTP port) for sending and receiving T.38 packets. <ul style="list-style-type: none"> ▪ [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: <ul style="list-style-type: none"> ▪ 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 T38UseRTPPort parameter 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 re-routing of Tel-to-IP calls that are identified as fax calls. <ul style="list-style-type: none"> ▪ [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 Outbound IP Routing Table is then used to route the call and the destination number manipulation mechanism is used to remove the "FAX" prefix, if required. <p>If the initial INVITE used to establish the voice call (not fax) was already sent, a CANCEL (if not connected yet) or a BYE (if already connected) is sent to tear down the voice call.</p> Notes: <ul style="list-style-type: none"> ▪ 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.
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. <ul style="list-style-type: none"> ▪ [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: <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ This parameters is applicable only if the parameter IsFaxUsed is

Parameter	Description
	set to 1 (T.38 Relay) or 3 (Fax Fallback).
[T38FaxSessionImmediate Start]	<p>Enables fax transmission of T.38 “no-signal” packets to the terminating fax machine.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>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.</p> <p>To overcome this, the device sends No-Op (“no-signal”) packets to open a pinhole in the NAT for the answering fax machine. The originating fax does not wait for an answer, but immediately starts sending T.38 packets to the terminating fax machine.</p> <p>Note: To enable No-Op packet transmission, use the NoOpEnable and NoOpInterval parameters.</p>

A.12.2 DTMF and Hook-Flash Parameters

The DTMF and hook-flash parameters are described in the table below.

Table A-38: DTMF and Hook-Flash Parameters

Parameter	Description
Hook-Flash Parameters	
Web/EMS: Hook-Flash Code [HookFlashCode]	<p>For analog interfaces: Defines the digit pattern that when received from the Tel side, indicates a Hook Flash event. For digital interfaces: Defines the digit pattern used by the PBX to indicate a Hook Flash event. When this pattern is detected from the Tel side, the device responds as if a Hook Flash event has occurred and sends a SIP INFO message if the HookFlashOption parameter is set to 1, 5, 6, or 7 (indicating a Hook Flash). If configured and a Hook Flash indication is received from the IP side, the device generates this pattern to the Tel side.</p> <p>The valid range is a 25-character string. The default is a null string.</p> <p>Note: This parameter can also be configured per Tel Profile, using the TelProfile parameter.</p>
Web/EMS: Hook-Flash Option [HookFlashOption]	<p>Determines the hook-flash transport type (i.e., method by which hook-flash is sent and received). For digital interfaces (E1/T1): This feature is applicable only if the HookFlashCode parameter is configured.</p> <ul style="list-style-type: none"> ▪ [0] Not Supported = Hook-Flash indication is not sent (default). ▪ [1] INFO = Sends proprietary INFO message (Broadsoft) with Hook-Flash indication. The device sends the INFO message as follows: <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> Content-Type: application/broadsoft; version=1.0 Content-Length: 17 event flashhook </div> ▪ [4] RFC 2833 = This option is currently not supported.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [5] INFO (Lucent) = Sends proprietary SIP INFO message with Hook-Flash indication. The device sends the INFO message as follows: Content-Type: application/hook-flash Content-Length: 11 signal=hf ▪ [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 <p>Notes:</p> <ul style="list-style-type: none"> ▪ The device can interwork DTMF HookFlashCode to SIP INFO messages with Hook Flash indication (for digital interfaces). ▪ 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 EnableHold parameter 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: <ul style="list-style-type: none"> ▪ 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).
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: <ul style="list-style-type: none"> ▪ FXS interfaces: <ul style="list-style-type: none"> ✓ 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: <ul style="list-style-type: none"> ▪ 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

Parameter	Description
	hook-flash, set this parameter to 550. <ul style="list-style-type: none"> This parameter can also be configured per Tel Profile, using the TelProfile parameter.
DTMF Parameters	
EMS: Use End of DTMF [MGCPDTMFDetectionPoint]	Determines when the detection of DTMF events is notified. <ul style="list-style-type: none"> [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. <ul style="list-style-type: none"> [0] No = Don't declare RFC 2833 telephony-event parameter in SDP. [3] Yes = Declare RFC 2833 telephony-event parameter in SDP (default). <p>The device is always receptive to RFC 2833 DTMF relay packets. Therefore, it is always correct to include the 'telephony-event' parameter as default in the SDP. However, some devices use the absence of the 'telephony-event' in the SDP to decide to send DTMF digits in-band using G.711 coder. If this is the case, you can set this parameter to 0.</p> <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see 'Configuring IP Profiles' on page 217).</p>
Tx DTMF Option Table	
Web/EMS: Tx DTMF Option [TxDTMFOption]	This parameter table configures up to two preferred transmit DTMF negotiation methods. The format of this parameter is as follows: [TxDTMFOption] FORMAT TxDTMFOption_Index = TxDTMFOption_Type; [TxDTMFOption] Where Type is: <ul style="list-style-type: none"> [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. <p>For example: TxDTMFOption 0 = 1; TxDTMFOption 1 = 3;</p> <p>Notes:</p> <ul style="list-style-type: none"> 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: <ol style="list-style-type: none"> Negotiates RFC 2833 payload type using local and remote

Parameter	Description
	<p>SDPs.</p> <ul style="list-style-type: none"> 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). <ul style="list-style-type: none"> ▪ When TxDTMFOption is set to 0, the RFC 2833 payload type is set according to the parameter RFC2833PayloadType for both transmit and receive. ▪ If an ISDN phone user presses digits (e.g., for interactive voice response / IVR applications such as retrieving voice mail messages), ISDN Information messages received by the device for each digit are sent in the voice channel to the IP network as DTMF signals, according to the settings of the TxDTMFOption parameter. ▪ The <i>ini</i> 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 217).
[DisableAutoDTMFMute]	<p>Enables the automatic muting of DTMF digits when out-of-band DTMF transmission is used.</p> <ul style="list-style-type: none"> ▪ [0] = Automatic mute is used (default). ▪ [1] = No automatic mute of in-band DTMF. <p>When this parameter is set to 1, the DTMF transport type is set according to the parameter DTMFTransportType and the DTMF digits aren't muted if out-of-band DTMF mode is selected (TxDTMFOption set to 1, 2 or 3). This enables the sending of DTMF digits in-band (transparent of RFC 2833) in addition to out-of-band DTMF messages.</p> <p>Note: Usually this mode is not recommended.</p>
<p>Web/EMS: Enable Digit Delivery to IP [EnableDigitDelivery2IP]</p>	<p>Enables the Digit Delivery feature whereby DTMF digits are sent to the destination IP address after the Tel-to-IP call is answered.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = Enable digit delivery to IP. <p>To enable this feature, modify the called number to include at least one 'p' character. The device uses the digits before the 'p' character in the initial INVITE message. After the call is answered, the device waits for the required time (number of 'p' multiplied by 1.5 seconds), and then sends the rest of the DTMF digits using the method chosen (in-band or out-of-band).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.
<p>Web: Enable Digit Delivery to Tel EMS: Enable Digit Delivery [EnableDigitDelivery]</p>	<p>Enables the Digit Delivery feature, which sends DTMF digits of the called number to the device's port (analog)/B-channel (digital) (phone line) after the call is answered (i.e., line is off-hooked for FXS, or seized for FXO) for IP-to-Tel calls.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = Enable Digit Delivery feature for the FXO/FXS device. <p>For digital interfaces: If the called number in IP-to-Tel call includes the characters 'w' or 'p', the device places a call with the first part of the</p>

Parameter	Description
	<p>called number (before 'w' or 'p') and plays DTMF digits after the call is answered. If the character 'w' is used, the device waits for detection of a dial tone before it starts playing DTMF digits. For example, if the called number is '1007766p100', the device places a call with 1007766 as the destination number, then after the call is answered it waits 1.5 seconds ('p') and plays the rest of the number (100) as DTMF digits.</p> <p>Additional examples: 1664wpp102, 66644ppp503, and 7774w100pp200.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ For analog interfaces: The called number can include characters 'p' (1.5 seconds pause) and 'd' (detection of dial tone). If character 'd' is used, it must be the first 'digit' in the called number. The character 'p' can be used several times. For example (for FXS/FXO interfaces), the called number can be as follows: d1005, dpp699, p9p300. To add the 'd' and 'p' digits, use the usual number manipulation rules. ▪ For analog interfaces: 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. ▪ For analog interfaces: 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.
<p>[ReplaceNumberSignWithEscapeChar]</p>	<p>Determines whether to replace the number sign (#) with the escape character (%23) in outgoing SIP messages for Tel-to-IP calls.</p> <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only if the parameter IsSpecialDigits is set 1. ▪ This parameter is applicable only to analog interfaces.
<p>Web: Special Digit Representation EMS: Use Digit For Special DTMF [UseDigitForSpecialDTMF]</p>	<p>Defines the representation for 'special' digits ('*' and '#') that are used for out-of-band DTMF signaling (using SIP INFO/NOTIFY).</p> <ul style="list-style-type: none"> ▪ [0] Special = Uses the strings '*' and '#' (default). ▪ [1] Numeric = Uses the numerical values 10 and 11.

A.12.3 Digit Collection and Dial Plan Parameters

The digit collection and dial plan parameters are described in the table below.

Table A-39: Digit Collection and Dial Plan Parameters

Parameter	Description
Web/EMS: Dial Plan Index [DialPlanIndex]	<p>Defines the Dial Plan index to use in the external Dial Plan file. The Dial Plan file is loaded to the device as a .dat file (converted using the DConvert utility). The Dial Plan index can be defined globally or per Tel Profile.</p> <p>The valid value range is 0 to 7, where 0 denotes PLAN1, 1 denotes PLAN2, and so on. The default is -1, indicating that no Dial Plan file is used.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 is applicable also to ISDN with overlap dialing. ▪ For E1 CAS MFC-R2 variants (which don't support terminating digit for the called party number, usually I-15), this parameter and the DigitMapping parameter are ignored. Instead, you can define a Dial Plan template per trunk using the parameter CasTrunkDialPlanName_x (or in the Trunk Settings page). ▪ This parameter can also be configured per Tel Profile, using the TelProfile parameter. ▪ For more information on the Dial Plan file, see 'External Dial Plan File' on page 335.
[Tel2IPSourceNumberMappingDialPlanIndex]	<p>Defines the Dial Plan index in the external Dial Plan file for the Tel-to-IP Source Number Mapping feature.</p> <p>The valid value range is 0 to 7, defining the Dial Plan index [Plan x] in the Dial Plan file. The default is -1 (disabled).</p> <p>For more information on this feature, see 'Modifying ISDN-to-IP Calling Party Number' on page 337.</p>
Web: Digit Mapping Rules EMS: Digit Map Patterns [DigitMapping]	<p>Defines the digit map pattern (used to reduce the dialing period when ISDN overlap dialing for digital interfaces). If the digit string (i.e., dialed number) matches one of the patterns in the digit map, the device stops collecting digits and establishes a call with the collected number.</p> <p>The digit map pattern can contain up to 52 options (rules), each separated by a vertical bar (). The maximum length of the entire digit pattern is 152 characters. The available notations include the following:</p> <ul style="list-style-type: none"> ▪ [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

Parameter	Description
	<p>99 998, then the digit collection is terminated after the first two 9 digits are received. Therefore, the second rule of 998 can never be matched. But when the digit map is 99s 998, then after dialing the first two 9 digits, the device waits another two seconds within which the caller can enter the digit 8.</p> <p>An example of a digit map is shown below: 11xS 00T [1-7]xxx 8xxxxxxx #xxxxxxx *xx 91xxxxxxxxx 9011x.T In the example above, the last rule can apply to International numbers: 9 for dialing tone, 011 Country Code, and then any number of digits for the local number ('x').</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For ISDN interfaces, the digit map mechanism is applicable only when ISDN overlap dialing is used (ISDNRxOverlap is set to 1). ▪ 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 more information on digit mapping, see 'Digit Mapping' on page 334.
Web: Max Digits in Phone Num EMS: Max Digits in Phone Number [MaxDigits]	<p>Defines the maximum number of collected destination number digits that can be received (i.e., dialed) from the Tel side (analog) when Tel-to-IP ISDN overlap dialing is performed (digital). When the number of collected digits reaches this maximum, the device uses these digits for the called destination number.</p> <p>The valid range is 1 to 49. The default value is 5 for analog and 30 for digital.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ Instead of using this parameter, Digit Mapping rules can be configured. ▪ Dialing ends when any of the following scenarios occur: <ul style="list-style-type: none"> ✓ 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]	<p>For analog interfaces: Defines the time (in seconds) that the device waits between digits that are dialed by the user.</p> <p>For ISDN overlap dialing: Defines the time (in seconds) that the device waits between digits that are received from the PSTN or IP during overlap dialing.</p> <p>When this inter-digit timeout expires, the device uses the collected digits to dial the called destination number.</p> <p>The valid range is 1 to 10. The default value is 4.</p>
Web: Enable Special Digits EMS: Use '#' For Dial Termination [IsSpecialDigits]	<p>Determines whether the asterisk (*) and pound (#) digits can be used in DTMF.</p> <ul style="list-style-type: none"> ▪ [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. <p>Note: These symbols can always be used as the first digit of a dialed number even if you disable this parameter.</p>

A.12.4 Voice Mail Parameters

The voice mail parameters are described in the table below. For more information on the Voice Mail application, refer to the *CPE Configuration Guide for Voice Mail*.

Table A-40: Voice Mail Parameters

Parameter	Description												
Web/EMS: Voice Mail Interface [VoiceMailInterface]	<p>Enables the device's Voice Mail application and determines the communication method used between the PBX and the device.</p> <ul style="list-style-type: none"> ▪ [0] None (default) ▪ [1] DTMF ▪ [2] SMDI ▪ [3] QSIG ▪ [4] SETUP Only = For ISDN ▪ [5] MATRA/AASTRA QSIG ▪ [6] QSIG SIEMENS = QSIG MWI activate and deactivate messages include Siemens Manufacturer Specific Information (MSI) ▪ [7] IP2IP = The device's IP2IP application is used for interworking between an IP Voice Mail server and the device. This is implemented for sending unsolicited SIP NOTIFY messages received from the Voice Mail server to an IP Group (configured using the parameter NotificationIPGroupID). ▪ [8] ETSI = Euro ISDN, according to ETS 300 745-1 V1.2.4, section 9.5.1.1. Enables MWI interworking from IP to Tel, typically used for BRI phones. <p>Note: To disable voice mail per Trunk Group, you can use a Tel Profile ID (using the TelProfile parameter) that is configured with the EnableVoiceMailDelay parameter to disabled (0). This eliminates the phenomenon of call delay on Trunks not implementing voice mail when voice mail is enabled using this global parameter.</p>												
Web: Enable VoiceMail URI EMS: Enable VMURI [EnableVMURI]	<p>Enables the interworking of target and cause for redirection from Tel to IP and vice versa, according to RFC 4468.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable. <p>Upon receipt of an ISDN Setup message with Redirect values, the device maps the Redirect phone number to the SIP 'target' parameter and the Redirect number reason to the SIP 'cause' parameter in the Request-URI.</p> <p>Redirecting Reason >> SIP Response Code</p> <table border="0"> <tr> <td>Unknown</td> <td>>> 404</td> </tr> <tr> <td>User busy</td> <td>>> 486</td> </tr> <tr> <td>No reply</td> <td>>> 408</td> </tr> <tr> <td>Deflection</td> <td>>> 487/480</td> </tr> <tr> <td>Unconditional</td> <td>>> 302</td> </tr> <tr> <td>Others</td> <td>>> 302</td> </tr> </table> <p>If the device receives a Request-URI that includes a 'target' and 'cause' parameter, the 'target' is mapped to the Redirect phone number and the 'cause' is mapped to the Redirect number reason.</p>	Unknown	>> 404	User busy	>> 486	No reply	>> 408	Deflection	>> 487/480	Unconditional	>> 302	Others	>> 302
Unknown	>> 404												
User busy	>> 486												
No reply	>> 408												
Deflection	>> 487/480												
Unconditional	>> 302												
Others	>> 302												

Parameter	Description
[WaitForBusyTime]	<p>Defines the time (in msec) that the device waits to detect busy and/or reorder tones. This feature is used for semi-supervised PBX call transfers (i.e., the LineTransferMode parameter is set to 2).</p> <p>The valid value range is 0 to 20000 (i.e., 20 sec). The default is 2000 (i.e., 2 sec).</p>
Web/EMS: Line Transfer Mode [LineTransferMode]	<p>Defines the call transfer method used by the device. This parameter is applicable to FXO call transfer as well as E1/T1 CAS call transfer if the TrunkTransferMode_x parameter is set to 3 (CAS Normal) or 1 (CAS NFA).</p> <ul style="list-style-type: none"> ▪ [0] None = IP (default). ▪ [1] Blind = PBX blind transfer: <ul style="list-style-type: none"> ✓ Analog (FXO): After receiving a SIP REFER message from the IP side, the device (FXO) sends a hook-flash to the PBX, dials the digits (that are received in the Refer-To header), and then immediately releases the line (i.e., on-hook). The PBX performs the transfer internally. ✓ E1/T1 CAS: When a SIP REFER message is received, the device performs a blind transfer, by performing a CAS wink, waiting a user-defined time (configured by the WaitForDialTime parameter), dialing the Refer-To number, and then releasing the call. The PBX performs the transfer internally. ▪ [2] Semi Supervised = PBX semi-supervised transfer: <ul style="list-style-type: none"> ✓ Analog (FXO): After receiving a SIP REFER message from the IP side, the device sends a hook-flash to the PBX, and then dials the digits (that are received in the Refer-To header). If no busy or reorder tones are detected (within the user-defined interval set by the WaitForBusyTime parameter), the device completes the call transfer by releasing the line. If these tones are detected, the transfer is cancelled, the device sends a SIP NOTIFY message with a failure reason in the NOTIFY body (such as 486 if busy tone detected), and generates an additional hook-flash toward the FXO line to restore connection to the original call. ✓ E1/T1 CAS: The device performs a CAS wink, waits a user-defined time (configured by the WaitForDialTime parameter), and then dials the Refer-To number. If during the user-defined interval set by the WaitForBusyTime parameter, no busy or reorder tones are detected, the device completes the call transfer by releasing the line. If during this interval, the device detects these tones, the transfer operation is cancelled, the device sends a SIP NOTIFY message with a failure reason (e.g., 486 if a busy tone is detected), and then generates an additional wink toward the CAS line to restore connection with the original call. ▪ [3] Supervised = PBX Supervised transfer: <ul style="list-style-type: none"> ✓ Analog (FXO): After receiving a SIP REFER message from the IP side, the device sends a hook-flash to the PBX, and then dials the digits (that are received in the Refer-To header). The device waits for connection of the transferred call and then completes the call transfer by releasing the line. If speech is not detected, the transfer is cancelled, the device sends a SIP NOTIFY message with a failure reason in the NOTIFY body (such as 486 if busy tone detected) and

Parameter	Description
	<p>generates an additional hook-flash toward the FXO line to restore connection to the original call.</p> <ul style="list-style-type: none"> ✓ E1/T1 CAS: The device performs a supervised transfer to the PBX. The device performs a CAS wink, waits a user-defined time (configured by the WaitForDialTime parameter), and then dials the Refer-To number. The device completes the call transfer by releasing the line only after detection of the transferred party answer. To enable answer supervision, you also need to do the following: <ol style="list-style-type: none"> 1) Enable voice detection (i.e., set the EnableVoiceDetection parameter to 1). 2) Set the EnabledSPIPMDetectors parameter to 1. 3) Install the IPMDetector DSP option Feature Key.
SMDI Parameters	
Web/EMS: Enable SMDI [SMDI]	<p>Enables Simplified Message Desk Interface (SMDI) interface on the device.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Normal serial (default) ▪ [1] Enable (Bellcore) ▪ [2] Ericsson MD-110 ▪ [3] NEC (ICS) <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Defines the time (in msec) that the device waits for an SMDI Call Status message before or after a Setup message is received. This parameter synchronizes the SMDI and analog CAS interfaces. 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.</p>
Message Waiting Indication (MWI) Parameters	
Web: MWI Off Digit Pattern EMS: MWI Off Code [MWIOffCode]	<p>Defines the digit code used by the device to notify the PBX that there are no messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string.</p>
Web: MWI On Digit Pattern EMS: MWI On Code [MWIONCode]	<p>Defines the digit code used by the device to notify the PBX of messages waiting for a specific extension. This code is added as prefix to the dialed number. The valid range is a 25-character string.</p>
Web: MWI Suffix Pattern EMS: MWI Suffix Code [MWISuffixCode]	<p>Defines the digit code used by the device as a suffix for 'MWI On Digit Pattern' and 'MWI Off Digit Pattern'. This suffix is added to the generated DTMF string after the extension number. The valid range is a 25-character string.</p>
Web: MWI Source Number EMS: MWI Source Name [MWISourceNumber]	<p>Defines the calling party's phone number used in the Q.931 MWI Setup message to PSTN. If not configured, the channel's phone number is used as the calling number.</p>

Parameter	Description
[MWISubscribeIPGroupID]	<p>Defines the IP Group ID used when subscribing to an MWI server. The 'The SIP Group Name' field value of the IP Group table is used as the Request-URI host name in the outgoing MWI SIP SUBSCRIBE message. The request is sent to the IP address defined for the Proxy Set that is associated with the IP Group. The Proxy Set's capabilities such as proxy redundancy and load balancing are also applied to the message.</p> <p>For example, if the 'SIP Group Name' field of the IP Group is set to "company.com", the device sends the following SUBSCRIBE message:</p> <pre>SUBSCRIBE sip:company.com...</pre> <p>Instead of:</p> <pre>SUBSCRIBE sip:10.33.10.10...</pre> <p>Note: If this parameter is not configured, the MWI SUBSCRIBE message is sent to the MWI server as defined by the MWIServerIP parameter.</p>
[NotificationIPGroupID]	<p>Defines the IP Group ID to which the device sends SIP NOTIFY MWI messages.</p> <p>Notes:</p> <ul style="list-style-type: none"> This is used for MWI Interrogation. For more information on the interworking of QSIG MWI to IP, see Message Waiting Indication on page 293. To determine the handling method of MWI Interrogation messages, use the MWIInterrogationType parameter.
[MWIQsigMsgCentredIDPartyNumber]	<p>Defines the Message Centred ID party number used for QSIG MWI messages. If not configured (default), the parameter is not included in MWI (activate and deactivate) QSIG messages. The value is a string.</p>
<p>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 <i>CPE Configuration Guide for Voice Mail</i>.</p>	
Web: Forward on Busy Digit Pattern (Internal) EMS: Digit Pattern Forward On Busy [DigitPatternForwardOnBusy]	<p>Defines the digit pattern used by the PBX to indicate 'call forward on busy' when the original call is received from an internal extension. The valid range is a 120-character string.</p>
Web: Forward on No Answer Digit Pattern (Internal) EMS: Digit Pattern Forward On No Answer [DigitPatternForwardOnNoAnswer]	<p>Defines the digit pattern used by the PBX to indicate 'call forward on no answer' when the original call is received from an internal extension. The valid range is a 120-character string.</p>
Web: Forward on Do Not Disturb Digit Pattern (Internal) EMS: Digit Pattern Forward On DND [DigitPatternForwardOnDND]	<p>Defines the digit pattern used by the PBX to indicate 'call forward on do not disturb' when the original call is received from an internal extension. The valid range is a 120-character string.</p>

Parameter	Description
Web: Forward on No Reason Digit Pattern (Internal) EMS: Digit Pattern Forward No Reason [DigitPatternForwardNoReason]	Defines the digit pattern used by the PBX to indicate 'call forward with no reason' when the original call is received from an internal extension. The valid range is a 120-character string.
Web: Forward on Busy Digit Pattern (External) EMS: VM Digit Pattern On Busy External [DigitPatternForwardOnBusyExt]	Defines the digit pattern used by the PBX to indicate 'call forward on busy' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Web: Forward on No Answer Digit Pattern (External) EMS: VM Digit Pattern On No Answer Ext [DigitPatternForwardOnNoAnswerExt]	Defines the digit pattern used by the PBX to indicate 'call forward on no answer' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Web: Forward on Do Not Disturb Digit Pattern (External) EMS: VM Digit Pattern On DND External [DigitPatternForwardOnDNDExt]	Defines the digit pattern used by the PBX to indicate 'call forward on do not disturb' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Web: Forward on No Reason Digit Pattern (External) EMS: VM Digit Pattern No Reason External [DigitPatternForwardNoReasonExt]	Defines the digit pattern used by the PBX to indicate 'call forward with no reason' when the original call is received from an external line (not an internal extension). The valid range is a 120-character string.
Web: Internal Call Digit Pattern EMS: Digit Pattern Internal Call [DigitPatternInternalCall]	Defines the digit pattern used by the PBX to indicate an internal call. The valid range is a 120-character string.
Web: External Call Digit Pattern EMS: Digit Pattern External Call [DigitPatternExternalCall]	Defines the digit pattern used by the PBX to indicate an external call. The valid range is a 120-character string.
Web: Disconnect Call Digit Pattern EMS: Tel Disconnect Code [TelDisconnectCode]	Defines a digit pattern that when received from the Tel side, indicates the device to disconnect the call. The valid range is a 25-character string.
Web: Digit To Ignore Digit Pattern EMS: Digit To Ignore [DigitPatternDigitToIgnore]	Defines a digit pattern that if received as Src (S) or Redirect (R) numbers is ignored and not added to that number. The valid range is a 25-character string.

A.12.5 Supplementary Services Parameters

This subsection describes the device's supplementary telephony services parameters.

A.12.5.1 Caller ID Parameters

The caller ID parameters are described in the table below.

Table A-41: Caller ID Parameters

Parameter	Description
Web: Caller ID Permissions Table EMS: SIP Endpoints > Caller ID	
[EnableCallerID]	<p>This parameter table 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_Module, EnableCallerID_Port; [EnableCallerID]</p> <p>Where,</p> <ul style="list-style-type: none"> ▪ IsEnabled: <ul style="list-style-type: none"> ✓ [0] Disable = disables Caller ID (default). ✓ [1] Enable = enables Caller ID generation (FXS) or detection (FXO). ▪ Module = Module number (where 1 depicts the module in Slot 1). ▪ Port = Port number (where 1 depicts Port 1 of a module). <p>For example: EnableCallerID 0 = 1,3,1; (caller ID enabled on Port 1 of Module 3) EnableCallerID 1 = 0,3,2; (caller ID disabled on Port 2 of Module 3)</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The indexing of this parameter starts at 0. ▪ 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 320. ▪ For configuring ini file table parameters, see Configuring ini File Table Parameters on page 84.
Web: Caller Display Information Table EMS: SIP Endpoints > Caller ID	
[CallerDisplayInfo]	<p>This parameter table 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 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_Module, CallerDisplayInfo_Port; [CallerDisplayInfo]</p> <p>Where,</p> <ul style="list-style-type: none"> ▪ DisplayString = Caller ID string (up to 18 characters).

Parameter	Description
	<ul style="list-style-type: none"> ▪ IsCidRestricted = <ul style="list-style-type: none"> ✓ [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. ▪ Module = Module number (where 1 depicts the module in Slot 1). ▪ Port = Port number (where 1 depicts Port 1 of a module). <p>For example: CallerDisplayInfo 0 = Susan C.,0,1,1; ("Susan C." is sent as the Caller ID for Port 1 of Module 1) CallerDisplayInfo 1 = Mark M.,0,1,2; ("Mark M." is sent as Caller ID for Port 2 of Module 1)</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The indexing of this ini file table parameter starts at 0. ▪ 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). ▪ 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 318. ▪ For configuring ini file table parameters, see Configuring ini File Table Parameters on page 84.
Web/EMS: Enable Caller ID [EnableCallerID]	Enables Caller ID. <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable. <p>If the Caller ID service is enabled, then for FXS interfaces, calling number and Display text (from IP) are sent to the device's port. For FXO interfaces, the Caller ID signal is detected and sent to IP in the SIP INVITE message (as 'Display' element). For information on the Caller ID table, see Configuring Caller Display Information on page 318. To disable/enable caller ID generation per port, see Configuring Call Forward on page 319.</p>
Web: Caller ID Type EMS: Caller id Types [CallerIDType]	Determines the standard used for detection (FXO) and generation (FXS) of Caller ID, and detection (FXO) / generation (FXS) of MWI (when specified) signals: <ul style="list-style-type: none"> ▪ [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

Parameter	Description																								
	<ul style="list-style-type: none"> ▪ [17] Standard Denmark = Caller ID and MWI ▪ [18] Standard India ▪ [19] Standard Brazil <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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. 																								
Web: Enable FXS Caller ID Category Digit For Brazil Telecom [AddCPCPrefix2BrazilCallerID]	<p>Enables the interworking of Calling Party Category (cpc) code from SIP INVITE messages to FXS Caller ID first digit.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>When this parameter is enabled, the device sends the Caller ID number (calling number) with the cpc code (received in the SIP INVITE message) to the device's FXS port. The cpc code is added as a prefix to the caller ID (after IP-to-Tel calling number manipulation). For example, assuming that the incoming INVITE contains the following From (or P-Asserted-Id) header:</p> <pre style="background-color: #f0f0f0; padding: 5px;">From:<sip:+551137077801;cpc=payphone@10.20.7.35>;tag=53700</pre> <p>The calling number manipulation removes "+55" (leaving 10 digits), and then adds the prefix 7, the cpc code for payphone user. Therefore, the Caller ID number that is sent to the FXS port, in this example is 71137077801.</p> <p>If the incoming INVITE message doesn't contain the 'cpc' parameter, nothing is added to the Caller ID number.</p> <table border="1" data-bbox="560 1536 1394 1973"> <thead> <tr> <th>CPC Value in Received INVITE</th> <th>CPC Code Prefixed to Caller ID (Sent to FXS Endpoint)</th> <th>Description</th> </tr> </thead> <tbody> <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> </tbody> </table>	CPC Value in Received INVITE	CPC Code Prefixed to Caller ID (Sent to FXS Endpoint)	Description	cpc=unknown	1	Unknown user	cpc=subscribe	1	-	cpc=ordinary	1	Ordinary user	cpc=priority	2	Pre-paid user	cpc=test	3	Test user	cpc=operator	5	Operator	cpc=data	6	Data call
CPC Value in Received INVITE	CPC Code Prefixed to Caller ID (Sent to FXS Endpoint)	Description																							
cpc=unknown	1	Unknown user																							
cpc=subscribe	1	-																							
cpc=ordinary	1	Ordinary user																							
cpc=priority	2	Pre-paid user																							
cpc=test	3	Test user																							
cpc=operator	5	Operator																							
cpc=data	6	Data call																							

Parameter	Description			
	<table border="1" data-bbox="560 293 1390 338"> <tr> <td data-bbox="560 293 837 338">cpc=payphone</td> <td data-bbox="837 293 1117 338">7</td> <td data-bbox="1117 293 1390 338">Payphone user</td> </tr> </table> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only to FXS interfaces. ▪ For this parameter to be enabled, you must also set the parameter EnableCallingPartyCategory to 1. 	cpc=payphone	7	Payphone user
cpc=payphone	7	Payphone user		
[EnableCallerIDTypeTwo]	<p>Disables the generation of Caller ID type 2 when the phone is off-hooked. Caller ID type 2 (also known as off-hook Caller ID) is sent to a currently busy telephone to display the caller ID of the waiting call.</p> <ul style="list-style-type: none"> ▪ [0] = Caller ID type 2 isn't played. ▪ [1] = Caller ID type 2 is played (default). 			
EMS: Caller ID Timing Mode [AnalogCallerIDTimingMode]	<p>Determines when Caller ID is generated.</p> <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Determines the Bellcore Caller ID sub-standard.</p> <ul style="list-style-type: none"> ▪ [0] = Between rings (default). ▪ [1] = Not ring related. <p>Note: For this parameter to take effect, a device reset is required.</p>			
EMS: ETSI Caller ID Type One Sub Standard [ETSICallerIDTypeOneSubStandard]	<p>Determines the ETSI FSK Caller ID Type 1 sub-standard (FXS only).</p> <ul style="list-style-type: none"> ▪ [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. <p>Note: For this parameter to take effect, a device reset is required.</p>			
Web: Asserted Identity Mode EMS: Asserted ID Mode [AssertedIdMode]	<p>Determines whether the SIP header P-Asserted-Identity or P-Preferred-Identity is used in the generated INVITE request for Caller ID (or privacy).</p> <ul style="list-style-type: none"> ▪ [0] Disabled = None (default) ▪ [1] Adding PAsserted Identity ▪ [2] Adding PPreferred Identity <p>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).</p> <p>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.</p> <p>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</p>			

Parameter	Description
	<p>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>.</p> <p>The 200 OK response can contain the connected party CallerID - Connected Number and Connected Name. For example, if the call is answered by the device, the 200 OK response includes the P-Asserted-Identity with Caller ID. The device interworks (in some ISDN variants), the Connected Party number and name from Q.931 Connect message to SIP 200 OK with the P-Asserted-Identity header. In the opposite direction, if the ISDN device receives a 200 OK with P-Asserted-Identity header, it interworks it to the Connected party number and name in the Q.931 Connect message, including its privacy.</p>
Web: Use Destination As Connected Number [UseDestinationAsConnectedNumber]	<p>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.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Notes:</p> <ul style="list-style-type: none"> ▪ If the received Q.931 Connect message contains a Connected Party Number, this number is used in the P-Asserted-Identity header in 200 OK response. ▪ 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 ISDN, CAS, and/or FXO interfaces.
Web: Caller ID Transport Type EMS: Transport Type [CallerIDTransportType]	<p>Determines the device's behavior for Caller ID detection.</p> <ul style="list-style-type: none"> ▪ [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/PSTN side and then erased from the voice stream (default). <p>Note: Caller ID detection is applicable only to FXO interfaces.</p>

A.12.5.2 Call Waiting Parameters

The call waiting parameters are described in the table below.

Table A-42: Call Waiting Parameters

Parameter	Description
Web/EMS: Enable Call Waiting [EnableCallWaiting]	<p>Determines whether Call Waiting is enabled.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable the Call Waiting service. ▪ [1] Enable = Enable the Call Waiting service (default). <p>If enabled, when an FXS interface receives a call on a busy endpoint, it responds with a 182 response (and not with a 486 busy). The device plays a call waiting indication signal. When hook-flash is detected, the device switches to the waiting call. The device that initiated the waiting call plays a Call Waiting Ringback tone to the calling party after a 182 response is received.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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. ▪ For analog interfaces: You can use the parameter table CallWaitingPerPort to enable Call Waiting per port. ▪ For information on the Call Waiting feature, see Call Waiting on page 292.
EMS: Send 180 For Call Waiting [Send180ForCallWaiting]	<p>Determines the SIP response code for indicating Call Waiting.</p> <ul style="list-style-type: none"> ▪ [0] = Use 182 Queued response to indicate call waiting (default). ▪ [1] = Use 180 Ringing response to indicate call waiting.
<p>Web: Call Waiting Table EMS: SIP Endpoints > Call Waiting</p>	
[CallWaitingPerPort]	<p>This parameter table configures call waiting per FXS port. The format of this parameter is as follows:</p> <pre>[CallWaitingPerPort] FORMAT CallWaitingPerPort_Index = CallWaitingPerPort_IsEnabled, CallWaitingPerPort_Module, CallWaitingPerPort_Port; [CallWaitingPerPort]</pre> <p>Where,</p> <ul style="list-style-type: none"> ▪ IsEnabled: <ul style="list-style-type: none"> ✓ [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. ▪ Port = Port number.

Parameter	Description
	<ul style="list-style-type: none"> ▪ Module = Module number. For example: CallWaitingPerPort 0 = 0,1,1; (call waiting disabled for Port 1 of Module 1) CallWaitingPerPort 1 = 1,1,2; (call waiting enabled for Port 2 of Module 1) Notes: <ul style="list-style-type: none"> ▪ This parameter is applicable only to FXS ports. ▪ 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 321. ▪ For a description on using ini file table parameters, see Configuring ini File Table Parameters on page 84.
Web: Number of Call Waiting Indications EMS: Call Waiting Number of Indications [NumberOfWaitingIndications]	Defines the 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.
Web: Time Between Call Waiting Indications EMS: Call Waiting Time Between Indications [TimeBetweenWaitingIndications]	Defines the 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 [TimeBeforeWaitingIndications]	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]	Defines the 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]	Defines the index of the first Call Waiting Tone in the CPT file. This feature enables the called party to distinguish between different call origins (e.g., external versus internal calls). There are three ways to use the distinctive call waiting tones: <ul style="list-style-type: none"> ▪ 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 parameter table. ▪ 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

Parameter	Description
	<p>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).</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable only to analog interfaces. It is assumed that all Call Waiting Tones are defined in sequence in the CPT file. SIP Alert-Info header examples: <ul style="list-style-type: none"> ✓ 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: <pre>INFO sip:06@192.168.13.2:5060 SIP/2.0 Via:SIP/2.0/UDP 192.168.13.40:5060;branch=z9hG4bK040066422630 From: <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</pre>

A.12.5.3 Call Forwarding Parameters

The call forwarding parameters are described in the table below.

Table A-43: Call Forwarding Parameters

Parameter	Description
Web: Enable Call Forward [EnableForward]	<p>Enables the Call Forwarding feature.</p> <ul style="list-style-type: none"> [0] Disable = Disable the Call Forward service. [1] Enable = Enable Call Forward service (using REFER) (default). <p>For FXS interfaces, the Call Forward table (FwdInfo parameter) must be defined to use the Call Forward service. The device uses REFER messages for call forwarding.</p> <p>Note: To use this service, the devices at both ends must support this option.</p>
Web: Call Forwarding Table EMS: SIP Endpoints > Call Forward	
[FwdInfo]	<p>This parameter table 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:</p> <pre>[FwdInfo] FORMAT FwdInfo_Index = FwdInfo_Type, FwdInfo_Destination,</pre>

Parameter	Description
	<p>FwdInfo_NoReplyTime, FwdInfo_Module, FwdInfo_Port; [\FwdInfo]</p> <p>Where,</p> <ul style="list-style-type: none"> ▪ Type = the scenario for forwarding the call: <ul style="list-style-type: none"> ✓ [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. ▪ Module = Module number (where 1 depicts the module in Slot 1). ▪ Port = Port number (where 1 depicts Port 1 of a module). <p>For example:</p> <ul style="list-style-type: none"> ▪ Below configuration forwards calls originally destined to Port 1 of Module 1 to "1001" upon On Busy: FwdInfo 0 = 1,1001,30,1,1; ▪ Below configuration forwards calls originally destined to Port 2 of Module 1 to an IP address upon On Busy: FwdInfo 1 = 1,2003@10.5.1.1,30,1,2; <p>Notes:</p> <ul style="list-style-type: none"> ▪ The indexing of this parameter starts at 0. ▪ Ensure that the Call Forward feature is enabled (default) for the settings of this table parameter to take effect. To enable Call 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 Outbound IP Routing Table' (Prefix ini file parameter). ▪ For configuring this table using the Web interface, see Configuring Call Forward on page 319. ▪ For configuring ini file table parameters, see Configuring ini File Table Parameters on page 84.
<p>Call Forward Reminder Ring Parameters</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ These parameters are applicable only to FXS interfaces. ▪ For a description of this feature, see Call Forward Reminder Ring on page 290. 	
Web: Enable NRT Subscription [EnableNRTSubscription]	Enables endpoint subscription for Ring reminder event notification feature. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Web: AS Subscribe IPGroupID	Defines the IP Group ID that contains the Application server for Subscription.

Parameter	Description
[ASSubscribeIPGroupID]	The valid value range is 1 to 8. The default is -1 (i.e., not configured).
Web: NRT Retry Subscription Time [NRTSubscribeRetryTime]	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.

A.12.5.4 Message Waiting Indication Parameters

The message waiting indication (MWI) parameters are described in the table below.

Table A-44: MWI Parameters

Parameter	Description
Web: Enable MWI EMS: MWI Enable [EnableMWI]	Enables Message Waiting Indication (MWI). <ul style="list-style-type: none"> [0] Disable = Disabled (default). [1] Enable = MWI service is enabled. Notes: <ul style="list-style-type: none"> 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 more information on MWI, see 'Message Waiting Indication' on page 293.
Web/EMS: MWI Analog Lamp [MWIAnalogLamp]	Enables the visual display of MWI. <ul style="list-style-type: none"> [0] Disable = Disable (default). [1] Enable = Enables visual MWI by supplying line voltage of approximately 100 VDC to activate the phone's lamp. Notes: <ul style="list-style-type: none"> 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]	Enables sending MWI information to the phone display. <ul style="list-style-type: none"> [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: <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> [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.

Parameter	Description
Web: MWI Server IP Address EMS: MWI Server IP [MWIServerIP]	Defines the MWI server's IP address. If provided, the device subscribes to this IP address. The MWI server address can be configured as a numerical IP address or as a domain name. If not configured, the Proxy IP address is used instead.
Web/EMS: MWI Server Transport Type [MWIServerTransportType]	Determines the transport layer used for outgoing SIP dialogs initiated by the device to the MWI server. <ul style="list-style-type: none"> ▪ [-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]	Defines the MWI subscription expiration time in seconds. The default is 7200 seconds. The range is 10 to 2,000,000.
Web: MWI Subscribe Retry Time EMS: Subscribe Retry Time [SubscribeRetryTime]	Defines the subscription retry time (in seconds) after last subscription failure. The default is 120 seconds. The range is 10 to 2,000,000.
Web: Subscription Mode [SubscriptionMode]	Determines the method the device uses to subscribe to an MWI server. <ul style="list-style-type: none"> ▪ [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]	Determines the ETSI Visual Message Waiting Indication (VMWI) Type 1 sub-standard. <ul style="list-style-type: none"> ▪ [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]	Determines the Bellcore VMWI sub-standard. <ul style="list-style-type: none"> ▪ [0] = Between rings (default). ▪ [1] = Not ring related. Note: For this parameter to take effect, a device reset is required.

A.12.5.5 Call Hold Parameters

The call hold parameters are described in the table below.

Table A-45: Call Hold Parameters

Parameter	Description
Web/EMS: Enable Hold [EnableHold]	<p>For digital interfaces: Enables interworking of the Hold/Retrieve supplementary service from PRI to SIP.</p> <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default) <p>For analog interfaces: 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.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For digital interfaces: To support interworking of the Hold/Retrieve supplementary service from SIP to ISDN (for QSIG and Euro ISDN), set the parameter EnableHold2ISDN to 1. ▪ For analog interfaces: 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 217).
Web/EMS: Hold Format [HoldFormat]	<p>Determines the format of the SDP in the Re-INVITE hold request.</p> <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ The device does not send any RTP packets when it is in hold state (for both hold formats). ▪ For digital interfaces: This parameter is applicable only to QSIG and Euro ISDN protocols.
Web/EMS:Held Timeout [HeldTimeout]	<p>Defines the time interval that the device allows for a call to remain on hold. If a Resume (un-hold Re-INVITE) message is received before the timer expires, the call is renewed. If this timer expires, the call is released (terminated).</p> <ul style="list-style-type: none"> ▪ [-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: CHRRTIMEOUT [CHRRTIMEOUT]	<p>Defines the duration (in seconds) that the Call Hold Reminder Ring is played. If a user hangs up while a call is still on hold or there is a call waiting, then the FXS interface immediately rings the extension for the duration specified by this parameter. If the user off-hooks the phone, the call becomes active.</p> <p>The valid range is 0 to 600. The default value is 30.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only to FXS interfaces. ▪ This Reminder Ring feature can be disabled using the DisableReminderRing parameter.
[DisableReminderRing]	Disables the reminder ring, which notifies the FXS user of a call on hold

Parameter	Description
	<p>or a waiting call when the phone is returned to on-hook position.</p> <ul style="list-style-type: none"> ▪ [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). <p>Note: This parameter is applicable only to FXS interfaces.</p>
[PlayDTMFduringHold]	<p>Determines whether the device sends DTMF signals (or DTMF SIP INFO message) when a call is on hold.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default). ▪ [1] = Enable - If the call is on hold, the device stops playing the Held tone (if it is played) and sends DTMF: <ul style="list-style-type: none"> ✓ To Tel side: plays DTMF digits according to the received SIP INFO message(s). (The stopped Held tone is not played again.) ✓ To IP side: sends DTMF SIP INFO messages to an IP destination if it detects DTMF digits from the Tel side.

A.12.5.6 Call Transfer Parameters

The call transfer parameters are described in the table below.

Table A-46: Call Transfer Parameters

Parameter	Description
Web/EMS: Enable Transfer [EnableTransfer]	<p>Enables the Call Transfer feature.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable the call transfer service. ▪ [1] Enable = The device responds to a REFER message with the Referred-To header to initiate a call transfer (default). <p>For analog interfaces: If the transfer service is enabled, the user can activate Transfer using hook-flash signaling. If this service is enabled, the remote party performs the call transfer.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Defines the string that is added as a prefix to the transferred/forwarded called number when the REFER/3xx message is received.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 (only for analog interfaces) number from the originally dialed number.
Web: Transfer Prefix IP 2 Tel [XferPrefixIP2Tel]	<p>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</p>

Parameter	Description
	<p>applicable to FXO/CAS blind transfer modes, i.e., LineTransferMode = 1, 2 or 3, and TrunkTransferMode = 1 or 3 (for CAS).</p> <p>The valid range is a string of up to 9 characters. The default is an empty string.</p> <p>Note: This parameter is also applicable to ISDN Blind Transfer, according to AT&T Toll Free Transfer Connect Service (TR 50075) "Courtesy Transfer-Human-No Data". To support this transfer mode, you need to configure the parameter XferPrefixIP2Tel to "*8" and the parameter TrunkTransferMode to 5.</p>
Web/EMS: Enable Semi-Attended Transfer [EnableSemiAttendedTransfer]	<p>Determines the device behavior when Transfer is initiated while in Alerting state.</p> <ul style="list-style-type: none"> ▪ [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.
Web: Blind EMS: Blind Transfer [KeyBlindTransfer]	<p>Defines the keypad sequence to activate blind transfer for established Tel-to-IP calls. The Tel user can perform blind transfer by dialing the KeyBlindTransfer digits, followed by a transferee destination number.</p> <p>After the KeyBlindTransfer DTMF digits sequence is dialed, the current call is put on hold (using a Re-INVITE message), a dial tone is played to the channel, and then the phone number collection starts.</p> <p>After the destination phone number is collected, it is sent to the transferee in a SIP REFER request in a Refer-To header. The call is then terminated and a confirmation tone is played to the channel. If the phone number collection fails due to a mismatch, a reorder tone is played to the channel.</p> <p>Note: For FXS/FXO interfaces, it is possible to configure whether the KeyBlindTransfer code is added as a prefix to the dialed destination number, by using the parameter KeyBlindTransferAddPrefix.</p>
EMS: Blind Transfer Add Prefix [KeyBlindTransferAddPrefix]	<p>Determines whether the device adds the Blind Transfer code (defined by the KeyBlindTransfer parameter) to the dialed destination number.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note: This parameter is applicable only to FXO and FXS interfaces.</p>
EMS: Blind Transfer Disconnect Timeout [BlindTransferDisconnectTimeout]	<p>Defines the duration (in milliseconds) for which the device waits for a disconnection from the Tel side after the Blind Transfer Code (KeyBlindTransfer) has been identified. When this timer expires, a SIP REFER message is sent toward the IP side. If this parameter is set to 0, the REFER message is immediately sent. The valid value range is 0 to 1,000,000. The default is 0.</p>
Web: QSIG Path Replacement Mode CLI: qsig-path-replacement-md [QSIGPathReplacementMode]	<p>Enables QSIG transfer for IP-to-Tel and Tel-to-IP calls.</p> <ul style="list-style-type: none"> ▪ [0] IP2QSIGTransfer = Enables IP-to-QSIG transfer. (default) ▪ [1] QSIG2IPTransfer = Enables QSIG-to-IP transfer.

Parameter	Description
[ReplaceTel2IPCallingNumTimeout]	<p>Defines the maximum duration (timeout) to wait between call Setup and Facility with Redirecting Number for replacing the calling number (for Tel-to-IP calls).</p> <p>The valid value range is 0 to 10,000 msec. The default is 0.</p> <p>The interworking of the received Setup message to a SIP INVITE is suspended when this parameter is set to any value greater than 0. This means that the redirecting number in the Setup message is not checked. When a subsequent Facility with Call Transfer Complete/Update is received with a non-empty Redirection Number, the Calling Number is replaced with the received redirect number in the sent INVITE message.</p> <p>If the timeout expires, the device sends the INVITE without changing the calling number.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The suspension of the INVITE message occurs for all calls. ▪ This parameter is applicable to QSIG.

A.12.5.7 Three-Way Conferencing Parameters

The three-way conferencing parameters are described in the table below.

Table A-47: Three-Way Conferencing Parameters

Parameter	Description
Web: Enable 3-Way Conference EMS: Enable 3 Way [Enable3WayConference]	<p>Enables the 3-Way Conference feature.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: 3-Way Conference Mode EMS: 3 Way Mode [3WayConferenceMode]	<p>Determines the mode of operation when the 3-Way Conference feature is used.</p> <ul style="list-style-type: none"> ▪ [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 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 sets up the conference call using its IP media channels. These channels are obtained from the IP media module (i.e., MPM module). Note that the device must be housed with MPM module(s) to support three-way conferencing. The device supports

Parameter	Description
	<p>up to five simultaneous, on-board three-way conference calls.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only to FXS and BRI interfaces. ▪ Three-way conferencing using an external conference server is supported only by FXS interfaces. ▪ The on-board 3-way conference mode is not supported by Mediant 600. ▪ When using an external conference server (options [0] or [1]), a conference call with up to six participants can be established.
Web: Establish Conference Code EMS: Establish Code [ConferenceCode]	<p>Defines the DTMF digit pattern, which upon detection generates the conference call when three-way conferencing is enabled (Enable3WayConference is set to 1). The valid range is a 25-character string. The default is "!" (Hook-Flash).</p> <p>Note: If the FlashKeysSequenceStyle parameter is set to 1 or 2, the setting of the ConferenceCode parameter is overridden.</p>
Web/EMS: Conference ID [ConferenceID]	<p>Defines the Conference Identification string (up to 16 characters). The default value is 'conf'.</p> <p>For 3-way conferencing using an external media server: The device uses this identifier in the Conference-initiating INVITE that is sent to the media server when Enable3WayConference is set to 1.</p> <p>When using the Mediant 1000 Media Processing Module (MPM): To join a conference, the INVITE URI must include the Conference ID string, preceded by the number of the participants in the conference, and terminated by a unique number.</p> <p>For example: INVITE sip:4MyConference1234@10.1.10.10. INVITE messages with the same URI join the same conference. For example: ConferenceID = MyConference.</p>

A.12.5.8 Emergency Call Parameters

The emergency call parameters are described in the table below.

Table A-48: Emergency Call Parameters

Parameter	Description
EMS: Enable 911 PSAP [Enable911PSAP]	<p>Enables the support for the E911 DID protocol, according to the Bellcore GR-350-CORE standard. This protocol defines signaling between E911 Tandem Switches and the PSAP, using analog loop-start lines. The FXO device can be installed instead of an E911 switch, connected directly to PSAP DID loop-start lines.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only to FXO interfaces. ▪ This parameter can also be configured per Tel Profile, using the TelProfile parameter.
Web/EMS: Emergency Numbers [EmergencyNumbers]	<p>Defines a list of "emergency" numbers.</p> <p>For FXS: When one of these numbers is dialed, the outgoing INVITE message includes the SIP Priority and Resource-Priority headers. If</p>

Parameter	Description
	<p>the user places the phone on-hook, the call is not disconnected. Instead, a Hold Re-INVITE request is sent to the remote party. Only if the remote party disconnects the call (i.e., a BYE is received) or a timer expires (set by the EmergencyRegretTimeout parameter) is the call terminated.</p> <p>For FXO, CAS, and ISDN: These emergency numbers are used for the preemption of E911 IP-to-Tel calls when there are unavailable or busy channels. In this scenario, the device terminates one of the busy channels and sends the emergency call to this channel. This feature is enabled by setting the CallPriorityMode parameter to 2 ("Emergency"). For a description of this feature, see 'Pre-empting Existing Call for E911 IP-to-Tel Call' on page 304.</p> <p>The list can include up to four different numbers, where each number can be up to four digits long. Example: EmergencyNumbers = '100','911','112'</p>
Web: Emergency Calls Regret Timeout EMS: Emergency Regret Timeout [EmergencyRegretTimeout]	<p>Defines the time (in minutes) that the device waits before tearing-down an emergency call (defined by the parameter EmergencyNumbers). Until this time expires, an emergency call can only be disconnected by the remote party, typically, by a Public Safety Answering Point (PSAP). The valid range is 1 to 30. The default value is 10.</p> <p>Note: This parameter is applicable only to FXS interfaces.</p>

A.12.5.9 Call Cut-Through Parameters

The call cut-through parameters are described in the table below.

Table A-49: Call Cut-Through Parameters

Parameter	Description
Web: Enable Calls Cut Through EMS: Cut Through [CutThrough]	<p>Enables FXS endpoints to receive incoming IP calls while the port is in off-hook state.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>If enabled, the FXS interface answers the call and 'cuts through' the voice channel if there is no other active call on the port, even if the port is in off-hook state.</p> <p>When the call is terminated (by the remote IP party), the device plays a reorder tone for a user-defined time (configured by the CutThroughTimeForReorderTone parameter) and is then ready to answer the next incoming call without on-hooking the phone.</p> <p>The waiting call is automatically answered by the device when the current call is terminated (configured by setting the parameter EnableCallWaiting to 1).</p> <p>Note: This feature is applicable only to FXS interfaces.</p>
[DigitalCutThrough]	<p>Enables PSTN CAS channels/endpoints to receive incoming IP calls even if the B-channels are in off-hook state.</p> <ul style="list-style-type: none"> ▪ [0] Disabled (default) ▪ [1] Enabled <p>When enabled, this feature operates as follows:</p> <ol style="list-style-type: none"> 1 A Tel-to-IP call is established (connected) by the device for a B-

Parameter	Description
	<p>channel.</p> <ol style="list-style-type: none"> 2 The device receives a SIP BYE (i.e., IP side ends the call) and plays a reorder tone to the PSTN side for the duration set by the <code>CutThroughTimeForReOrderTone</code> parameter. The device releases the call towards the IP side (sends a SIP 200 OK). 3 The PSTN side, for whatever reason, remains off-hook. 4 If a new IP call is received for this B-channel after the reorder tone has ended, the device “cuts through” the channel and connects the call immediately (despite the B-channel being in physical off-hook state) without playing a ring tone. If an IP call is received while the reorder tone is played, the device rejects the call. <p>Notes:</p> <ul style="list-style-type: none"> ▪ If this parameter is disabled and the PSTN side remains in off-hook state after the IP call ends the call, the device releases the call after 60 seconds. ▪ A special CAS table can be used to report call status events (Active/Idle) to the PSTN side during Cut Through mode. ▪ The Digital Cut-Through feature can also be configured as a Tel Profile (using the <code>TelProfile</code> parameter) and therefore, assigned to specific B-channels that use specific CAS tables.

A.12.5.10 Automatic Dialing Parameters

The automatic dialing upon off-hook parameters are described in the table below.

Table A-50: Automatic Dialing Parameters

Parameter	Description
<p>Web: Automatic Dialing Table EMS: SIP Endpoints > Auto Dial</p>	
[TargetOfChannel]	<p>This <i>parameter</i> table 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:</p> <pre>[TargetOfChannel] FORMAT TargetOfChannel_Index = TargetOfChannel_Destination, TargetOfChannel_Type, TargetOfChannel_Module, TargetOfChannel_Port, TargetOfChannel_HotLineToneDuration; [TargetOfChannel]</pre> <p>Where,</p> <ul style="list-style-type: none"> ▪ Destination = Destination phone number that you want dialed. ▪ Type: <ul style="list-style-type: none"> ✓ [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 <code>HotLineToneDuration</code>), the destination phone number is automatically dialed. ▪ Module = Module number (where 1 depicts the module in Slot 1).

Parameter	Description
	<ul style="list-style-type: none"> Port = Port number (where 1 depicts the Port 1 of the module). 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. <p>For example, the below configuration defines automatic dialing of phone number 911 when the phone that is connected to Port 1 of Module 1 is off-hooked for over 10 seconds: TargetOfChannel 0 = 911, 1, 1, 1, 10; (phone number "911" is automatically dialed for Port 1 of Module 1 after being off-hooked for 10 seconds)</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable to FXS and FXO interfaces. The indexing of this <i>ini</i> file table parameter starts at 0. Define this parameter for each device port that implements Automatic Dialing. 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 317. For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.12.5.11 Direct Inward Dialing Parameters

The Direct Inward Dialing (DID) parameters are described in the table below.

Table A-51: DID Parameters

Parameter	Description
Web/EMS: Enable DID Wink [EnableDIDWink]	Enables Direct Inward Dialing (DID) using Wink-Start signaling. <ul style="list-style-type: none"> [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). <p>Note: This parameter can also be configured per Tel Profile, using the TelProfile parameter.</p>
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. <p>Note: This parameter is applicable only to FXS interfaces.</p>
EMS: NTT DID Signalling Form	Determines the type of DID signaling support for NTT (Japan) modem: DTMF- or Frequency Shift Keying (FSK)-based signaling. The devices

Parameter	Description
[NTTDIDSignallingForm]	<p>can be connected to Japan's NTT PBX using 'Modem' DID lines. These DID lines are used to deliver a called number to the PBX.</p> <ul style="list-style-type: none"> ▪ [0] = FSK-based signaling (default) ▪ [1] = DTMF-based signaling <p>Note: This parameter is applicable only to FXS interfaces.</p>
<p>EMS: Enable DID [EnableDID]</p>	<p>This <i>parameter table</i> enables support for Japan NTT 'Modem' DID. FXS interfaces can be connected to Japan's NTT PBX using 'Modem' DID lines. These DID lines are used to deliver a called number to the PBX. The DID signal can be sent alone or combined with an NTT Caller ID signal.</p> <p>The format of this parameter is as follows: [EnableDID] FORMAT EnableDID_Index = EnableDID_IsEnable, EnableDID_Port, EnableDID_Module; [EnableDID]</p> <p>Where,</p> <ul style="list-style-type: none"> ▪ IsEnable = Enables [1] or disables [0] (default) Japan NTT Modem DID support. ▪ Port = Port number. ▪ Module = Module number. <p>For example: EnableDID 0 = 1,1,2; (DID is enabled on Port 1 of Module 2)</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only to FXS interfaces. ▪ For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
[WinkTime]	<p>Defines the time (in msec) elapsed between two consecutive polarity reversals. This parameter can be used for DID signaling, for example, E911 lines to the Public Safety Answering Point (PSAP), according to the Bellcore GR-350-CORE standard (refer to the ini file parameter Enable911PSAP).</p> <p>The valid range is 0 to 4,294,967,295. The default is 200.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable to FXS and FXO interfaces. ▪ For this parameter to take effect, a device reset is required.

A.12.5.12 MLPP Parameters

The Multilevel Precedence and Preemption (MLPP) parameters are described in the table below.

Table A-52: MLPP Parameters

Parameter	Description
Web/EMS: Call Priority Mode [CallPriorityMode]	Enables priority calls handling. <ul style="list-style-type: none"> ▪ [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, for example, 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 Trunk Group for which the E911 call was initially destined and if the channel select mode (configured by the ChannelSelectMode parameter) is set to other than "By Dest Number" (0). The preemption is done only if the incoming IP-to-Tel call is identified as an emergency call. The device identifies emergency calls by one of the following: <ul style="list-style-type: none"> ✓ 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. <p>Notes:</p> <ul style="list-style-type: none"> ✓ Applicable to FXS/FXO, CAS, and ISDN interfaces. ✓ For FXO interfaces, the preemption is done only on existing IP-to-Tel calls. In other words, if all the current FXO channels are busy with calls that were initiated by the FXO (i.e., Tel-to-IP calls), new incoming emergency IP-to-Tel calls are dropped. ✓ For more information, see 'Pre-empting Existing Call for E911 IP-to-Tel Call' on page 304.
Web: MLPP Default Namespace EMS: Default Name Space [MLPPDefaultNamespace]	Determines the namespace used for MLPP calls received from the ISDN side and destined for the Application server. The namespace value is not present in the Precedence IE of the PRI Setup message. Therefore, the value is used in the Resource-Priority header of the outgoing SIP INVITE request. <ul style="list-style-type: none"> ▪ [1] DSN = DSN (default) ▪ [2] DOD = DOD ▪ [3] DRSN = DRSN ▪ [5] UC = UC
Web/EMS: Default Call Priority [SIPDefaultCallPriority]	Determines the default call priority for MLPP calls. <ul style="list-style-type: none"> ▪ [0] 0 = ROUTINE (default) ▪ [2] 2 = PRIORITY

Parameter	Description
	<ul style="list-style-type: none"> ▪ [4] 4 = IMMEDIATE ▪ [6] 6 = FLASH ▪ [8] 8 = FLASH-OVERRIDE ▪ [9] 9 = FLASH-OVERRIDE-OVERRIDE <p>If the incoming SIP INVITE request doesn't contain a valid priority value in the SIP Resource-Priority header, the default value is used in the Precedence IE (after translation to the relevant ISDN Precedence value) of the outgoing PRI Setup message.</p> <p>If the incoming PRI Setup message doesn't contain a valid Precedence Level value, the default value is used in the Resource-Priority header of the outgoing SIP INVITE request. In this scenario, the character string is sent without translation to a numerical value.</p>
Web: MLPP DiffServ EMS: Diff Serv [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 and outgoing MLPP calls with the Resource-Priority header. The valid range is 0 to 63. The default value is 50.
Web/EMS: Preemption Tone Duration [PreemptionToneDuration]	Defines the duration (in seconds) in which the device plays a preemption tone to the Tel and IP sides if a call is preempted. The valid range is 0 to 60. The default is 3. Note: If set to 0, no preemption tone is played.
Web: MLPP Normalized Service Domain EMS: Normalized Service Domain [MLPPNormalizedServiceDomain]	Defines the MLPP normalized service domain string. If the device receives an MLPP ISDN incoming call, it uses the parameter (if different from 'FFFFFF') as a Service domain in the SIP Resource-Priority header in outgoing INVITE messages. If the parameter is configured to 'FFFFFF', the Resource-Priority header is set to the MLPP Service Domain obtained from the Precedence IE. The valid value is 6 hexadecimal digits. The default is '000000'. Note: This parameter is applicable only to the MLPP NI-2 ISDN variant with CallPriorityMode set to 1.
[MLPPNetworkIdentifier]	Defines the MLPP network identifier (i.e., International prefix or Telephone Country Code/TCC) for IP-to-ISDN calls, according to the UCR 2008 and ITU Q.955 specifications. The valid range is 1 to 999. The default is 1 (i.e., USA). The MLPP network identifier is sent in the Facility IE of the ISDN Setup message. For example: <ul style="list-style-type: none"> ▪ MLPPNetworkIdentifier set to default (i.e., USA, 1): PlaceCall- MLPPNetworkID:0100 MlppServiceDomain:123abc, MlppPrecLevel:5 Fac(1c): 91 a1 15 02 01 05 02 01 19 30 0d 0a 01 05 0a 01 01 04 05 01 00 12 3a bc ▪ MLPPNetworkIdentifier set to 490: PlaceCall- MLPPNetworkID:9004 MlppServiceDomain:123abc, MlppPrecLevel:5 Fac(1c): 91 a1 15 02 01 0a 02 01 19 30 0d 0a 01 05 0a 01 01 04 05 90 04 12 3a bc
Web: MLPP Default Service Domain EMS: Default Service Domain	Defines the MLPP default service domain string. If the device receives a non-MLPP ISDN incoming call (without a Precedence IE), it uses the parameter (if different than "FFFFFF") as a Service

Parameter	Description
[MLPPDefaultServiceDomain]	<p>domain in the SIP Resource-Priority header in outgoing (Tel-to-IP calls) INVITE messages. This parameter is used in conjunction with the parameter SIPDefaultCallPriority.</p> <p>If MLPPDefaultServiceDomain is set to 'FFFFFF', the device interworks the non-MLPP ISDN call to non-MLPP SIP call, and the outgoing INVITE does not contain the Resource-Priority header.</p> <p>The valid value is a 6 hexadecimal digits. The default is "000000".</p> <p>Note: This parameter is applicable only to the MLPP NI-2 ISDN variant with CallPriorityMode set to 1.</p>
Web/EMS: Precedence Ringing Type [PrecedenceRingingType]	<p>Defines the index of the Precedence Ringing tone in the Call Progress Tones (CPT) file. This tone is used when the parameter CallPriorityMode is set to 1 and a Precedence call is received from the IP side.</p> <p>The valid range is -1 to 16. The default value is -1 (i.e., plays standard Ringing tone).</p> <p>Note: This parameter is applicable only to analog interfaces.</p>
EMS: E911 MLPP Behavior [E911MLPPBehavior]	<p>Defines the E911 (or Emergency Telecommunication Services/ETS) MLPP Preemption mode:</p> <ul style="list-style-type: none"> ▪ [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. <p>Note: This parameter is applicable only to analog interfaces.</p>
[RPRequired]	<p>Determines whether the SIP resource-priority tag is added in the SIP Require header of the INVITE message for Tel-to-IP calls.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Excludes the SIP resource-priority tag from the SIP Require header. ▪ [1] Enable (default) = Adds the SIP resource-priority tag in the SIP Require header. <p>Note: This parameter is applicable only to MLPP priority call handling (i.e., only when the CallPriorityMode parameter is set to 1).</p>

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

Parameter	Description
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).
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).

A.12.5.13 ISDN BRI Parameters

The automatic dialing upon off-hook parameters are described in the table below.

Table A-53: Automatic Dialing Parameters

Parameter	Description
Web: ISDN Supp Services Table	
[ISDNSuppServ]	<p>This <i>parameter</i> table defines BRI phone extension numbers per BRI port and configures various ISDN supplementary services per BRI endpoint. The format of this parameter is as follows:</p> <pre>[ISDNSuppServ] FORMAT ISDNSuppServ_Index = ISDNSuppServ_PhoneNumber, ISDNSuppServ_Module, ISDNSuppServ_Port, ISDNSuppServ_UserId, ISDNSuppServ_UserPassword, ISDNSuppServ_CallerID, ISDNSuppServ_IsPresentationRestricted, ISDNSuppServ_IsCallerIDEnabled; [\ISDNSuppServ]</pre> <p>For example: ISDNSuppServ 0 = 400, 1, 1, user, pass, callerid, 0, 1; ISDNSuppServ 1 = 401, 1, 1, user, pass, callerid, 0, 1;</p> <p>Notes:</p> <ul style="list-style-type: none"> For a description of each table parameter and for configuring the table using the Web interface, see 'Configuring ISDN Supplementary Services' on page 307. For configuring ini file table parameters, see 'Configuring ini File Table Parameters' on page 84.
BRI-to-SIP Supplementary Services Codes for Call Forward	
<p>Note: Upon receipt of an ISDN Facility message for call forward from the BRI phone, the device sends a SIP INVITE to the softswitch with a user-defined code in the SIP To header, representing the reason for the call forward. For more information on BRI call forwarding, see 'BRI Call Forwarding' on page 291.</p>	
Call Forward Unconditional [SuppServCodeCFU]	<p>Defines the prefix code for activating Call Forward Unconditional sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p>Note: The string must be enclosed in single apostrophe (e.g., '*72').</p>
Call Forward Unconditional Deactivation [SuppServCodeCFUDeact]	<p>Defines the prefix code for deactivating Call Forward Unconditional Deactivation sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p>Note: The string must be enclosed in single apostrophe (e.g., '*72').</p>
Call Forward on Busy [SuppServCodeCFB]	<p>Defines the prefix code for activating Call Forward on Busy sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p>Note: The string must be enclosed in single apostrophe (e.g., '*72').</p>
Call Forward on Busy Deactivation [SuppServCodeCFBDeact]	<p>Defines the prefix code for deactivating Call Forward on Busy Deactivation sent to the softswitch.</p> <p>The valid value is a string. The default is an empty string.</p> <p>Note: The string must be enclosed in single apostrophe (e.g., '*72').</p>

Parameter	Description
Call Forward on No Reply [SuppServCodeCFNR]	Defines the prefix code for activating Call Forward on No Reply sent to the softswitch. The valid value is a string. The default is an empty string. Note: The string must be enclosed in single apostrophe (e.g., '*72').
Call Forward on No Reply Deactivation [SuppServCodeCFNRDeact]	Defines the prefix code for deactivating Call Forward on No Reply Deactivation sent to the softswitch. The valid value is a string. The default is an empty string. Note: The string must be enclosed in single apostrophe (e.g., '*72').

A.12.5.14 TTY/TDD Parameters

The TTY (telephone typewriter) or telecommunications device for the deaf (TDD) is an electronic device for text communication via a telephone line for those with impaired hearing. The TTY/TDD parameters are described in the table below.

Table A-54: TTY Parameters

Parameter	Description
[TTYTransportType]	Defines the device's transferring method of TTY signals during a call. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [2] = Relay (signals sent over the EVRC codec) - TTY phone device transfer using In-Band Relay mode for TTY signal transport. Note: To support TTY Relay (2), you must configure the device to use the EVRC coder.

A.12.6 PSTN Parameters

This subsection describes the device's PSTN parameters.

A.12.6.1 General Parameters

The general PSTN parameters are described in the table below.

Table A-55: General PSTN Parameters

Parameter	Description
Web/EMS: Protocol Type [ProtocolType]	<p>Defines the PSTN protocol for all the Trunks. To configure the protocol type for a specific Trunk, use the <i>ini</i> file parameter ProtocolType_x:</p> <ul style="list-style-type: none"> ▪ [0] NONE ▪ [1] E1 EURO ISDN = ISDN PRI Pan-European (CTR4) protocol ▪ [2] T1 CAS = Common T1 robbed bits protocols including E&M wink start, E&M immediate start, E&M delay dial/start and loop-start and ground start. ▪ [3] T1 RAW CAS ▪ [4] T1 TRANSPARENT = Transparent protocol, where no signaling is provided by the device. Timeslots 1 to 24 of all trunks are mapped to DSP channels. ▪ [5] E1 TRANSPARENT 31 = Transparent protocol, where no signaling is provided by the device. Timeslots 1 to 31 of each trunk are mapped to DSP channels. ▪ [6] E1 TRANSPARENT 30 = Transparent protocol, where no signaling is provided by the device. Timeslots 1 to 31, excluding time slot 16 of all trunks are mapped to DSP channels. ▪ [7] E1 MFCR2 = Common E1 MFC/R2 CAS protocols (including line signaling and compelled register signaling). ▪ [8] E1 CAS = Common E1 CAS protocols (including line signaling and MF/DTMF address transfer). ▪ [9] E1 RAW CAS ▪ [10] T1 NI2 ISDN = National ISDN 2 PRI protocol ▪ [11] T1 4ESS ISDN = ISDN PRI protocol for the Lucent™/AT&T™ 4ESS switch. ▪ [12] T1 5ESS 9 ISDN = ISDN PRI protocol for the Lucent™/AT&T™ 5ESS-9 switch. ▪ [13] T1 5ESS 10 ISDN = ISDN PRI protocol for the Lucent™/AT&T™ 5ESS-10 switch. ▪ [14] T1 DMS100 ISDN = ISDN PRI protocol for the Nortel™ DMS switch. ▪ [15] J1 TRANSPARENT ▪ [16] T1 NTT ISDN = ISDN PRI protocol for the Japan - Nippon Telegraph Telephone (known also as INS 1500). ▪ [17] E1 AUSTEL ISDN = ISDN PRI protocol for the Australian Telecom. ▪ [18] E1 HKT ISDN = ISDN PRI (E1) protocol for the Hong Kong - HKT. ▪ [19] E1 KOR ISDN = ISDN PRI protocol for Korean Operator (similar to ETSI). ▪ [20] T1 HKT ISDN = ISDN PRI (T1) protocol for the Hong Kong

Parameter	Description
	<p>- HKT.</p> <ul style="list-style-type: none"> ▪ [21] E1 QSIG = ECMA 143 QSIG over E1 ▪ [22] E1 TNZ = ISDN PRI protocol for Telecom New Zealand (similar to ETSI) ▪ [23] T1 QSIG = ECMA 143 QSIG over T1 ▪ [30] E1 FRENCH VN6 ISDN = France Telecom VN6 ▪ [31] E1 FRENCH VN3 ISDN = France Telecom VN3 ▪ [34] T1 EURO ISDN = ISDN PRI protocol for Euro over T1 ▪ [35] T1 DMS100 Meridian ISDN = ISDN PRI protocol for the Nortel™ DMS Meridian switch ▪ [36] T1 NI1 ISDN = National ISDN 1 PRI protocol ▪ [40] E1 NI2 ISDN = National ISDN 2 PRI protocol over E1 ▪ [50] BRI EURO ISDN = Euro ISDN over BRI ▪ [54] BRI QSIG = QSIG over BRI ▪ [55] BRI FRENCH VN6 ISDN = VN6 over BRI ▪ [56] BRI NTT = BRI ISDN Japan (Nippon Telegraph) <p>Notes:</p> <ul style="list-style-type: none"> ▪ All PRI trunks must be configured as the same line type (either E1 or T1). The device can support different variants of CAS and PRI protocols on different E1/T1 spans (no more than four simultaneous PRI variants). ▪ BRI trunks can operate with E1 or T1 trunks.
[ProtocolType_x]	<p>Defines the protocol type for a specific trunk ID (where x denotes the Trunk ID and 0 is the first trunk). For more information, see the ProtocolType parameter.</p>
[ISDNTimerT310]	<p>Defines the T310 override timer for DMS, Euro ISDN, and ISDN NI2 variants. An ISDN timer is started when a Q.931 Call Proceeding message is received. The timer is stopped when a Q.931 Alerting, Connect, or Disconnect message is received from the other end. If no ISDN Alerting, Progress, or Connect message is received within the duration of T310 timer, the call clears. The valid value range is 0 to 600 seconds. The default is 0 (i.e., use the default timer value according to the protocol's specifications).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ When both the parameters ISDNDmsTimerT310 and ISDNTimerT310 are configured, the value of the parameter ISDNTimerT310 prevails.
[ISDNDMSTimerT310]	<p>Overrides the T310 timer for the DMS-100 ISDN variant. T310 defines the timeout between the receipt of a Proceeding message and the receipt of an Alerting/Connect message. The valid range is 10 to 30. The default value is 10 (seconds).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ Instead of configuring this parameter, it is recommended to use the parameter ISDNTimerT310. ▪ This parameter is applicable only to Nortel DMS and Nortel MERIDIAN PRI variants (ProtocolType = 14 and 35).
[ISDNJapanNTTTimerT3JA]	<p>Defines the T3_JA timer (in seconds). This parameter overrides the internal PSTN T301 timeout on the Users Side (TE side).</p>

Parameter	Description
	If an outgoing call from the device to ISDN is not answered during this timeout, the call is released. The valid range is 10 to 240. The default value is 50. Notes: <ul style="list-style-type: none"> ▪ This timer is also affected by the parameter PSTNAlertTimeout. ▪ This parameter is applicable only to the Japan NTT PRI variant (ProtocolType = 16).
Web/EMS: Trace Level [TraceLevel]	Defines the trace level: <ul style="list-style-type: none"> ▪ [0] No Trace (default) ▪ [1] Full ISDN Trace ▪ [2] Layer 3 ISDN Trace ▪ [3] Only ISDN Q.931 Messages Trace ▪ [4] Layer 3 ISDN No Duplication Trace
Web/EMS: Framing Method [FramingMethod]	Determines the physical framing method for the trunk. <ul style="list-style-type: none"> ▪ [0] Extended Super Frame = (Default) Depends on protocol type: <ul style="list-style-type: none"> ✓ E1: E1 CRC4 MultiFrame Format extended G.706B (same as c) ✓ T1: T1 Extended Super Frame with CRC6 (same as D) ▪ [1] Super Frame = T1 SuperFrame Format (as B). ▪ [a] E1 FRAMING DDF = E1 DoubleFrame Format - CRC4 is forced to off ▪ [b] E1 FRAMING MFF CRC4 = E1 CRC4 MultiFrame Format - CRC4 is always on ▪ [c] E1 FRAMING MFF CRC4 EXT = E1 CRC4 MultiFrame Format extended G.706B - auto negotiation is on. If the negotiation fails, it changes automatically to CRC4 off (ddf) ▪ [A] T1 FRAMING F4 = T1 4-Frame multiframe. ▪ [B] T1 FRAMING F12 = T1 12-Frame multiframe (D4). ▪ [C] T1 FRAMING ESF = T1 Extended SuperFrame without CRC6 ▪ [D] T1 FRAMING ESF CRC6 = T1 Extended SuperFrame with CRC6 ▪ [E] T1 FRAMING F72 = T1 72-Frame multiframe (SLC96) ▪ [F] T1 FRAMING ESF CRC6 J2 = J1 Extended SuperFrame with CRC6 (Japan) Note: This parameter is not configurable for BRI interfaces; the device automatically uses the BRI framing method.
[FramingMethod_x]	Same as the description for parameter FramingMethod, but for a specific trunk ID (where x denotes the Trunk ID and 0 is the first Trunk).
Web/EMS: Clock Master [ClockMaster]	Determines the Tx clock source of the E1/T1 line. <ul style="list-style-type: none"> ▪ [0] Recovered = Generate the clock according to the Rx of the E1/T1 line (default). ▪ [1] Generated = Generate the clock according to the internal TDM bus. Notes: <ul style="list-style-type: none"> ▪ The source of the internal TDM bus clock is determined by the parameter TDMBusClockSource.

Parameter	Description
[ClockMaster_x]	Same as the description for parameter ClockMaster, but for a specific Trunk ID (where x denotes the Trunk ID and 0 is the first Trunk).
Web/EMS: Line Code [LineCode]	<p>Selects B8ZS or AMI for T1 spans, and HDB3 or AMI for E1 spans.</p> <ul style="list-style-type: none"> ▪ [0] B8ZS = use B8ZS line code (for T1 trunks only) default. ▪ [1] AMI = use AMI line code. ▪ [2] HDB3 = use HDB3 line code (for E1 trunks only). <p>Note: This parameter is not configurable for BRI interfaces; the device automatically uses the Modified Alternate Mark Invert (MAMI) line code.</p>
[LineCode_x]	Same as the description for parameter LineCode, but for a specific trunk ID (where 0 depicts the first trunk).
[TrunkLifeLineType]	<p>Determines the scenarios upon which the PSTN Fallback (lifeline) feature is activated. This feature redirects IP calls to the PSTN upon a power outage, a LAN disconnection, or lack of IP connectivity (i.e., no ping), thereby guaranteeing call continuity. PSTN Fallback is supported if the device houses one or two E1/T1 ("TRUNKS") modules, where each module provides two or four spans. In the event of a PSTN fallback, the module's metallic relay switch automatically connects trunk Port 1 (I) to Port 2 (II), and / or trunk Port 3 (III) to Port 4 (IIII), of the same module.</p> <p>Therefore, if for example, a PBX trunk is connected to Port 1 and the PSTN network is connected to Port 2, when PSTN fallback is activated, calls from the PBX are routed directly to the PSTN through Port 2.</p> <ul style="list-style-type: none"> ▪ [0] = Activate PSTN Fallback upon power outage (default). ▪ [1] = Activate PSTN Fallback upon power outage or detection of LAN disconnection. ▪ [2] = Activate PSTN Fallback on power outage, detection of LAN disconnection, or loss of ping (i.e., no IP connectivity). <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ PSTN Fallback is supported only between ports on the same module. ▪ PSTN Fallback is supported only for ISDN when the number of supported channels (e.g., 30) is less than the maximum number of possible channels provided by the physical ports (e.g., two E1 trunks). When the number of supported channels (e.g., 60) equals the maximum number of channels provided by the physical ports (e.g., two E1 trunks), then other protocols such as CAS are also supported. ▪ The PSTN Fallback feature has no relation to the PSTN Fallback Software Upgrade Key.
[AdminState]	<p>Defines the administrative state for all trunks.</p> <ul style="list-style-type: none"> ▪ [0] = Lock the trunk; stops trunk traffic to configure the trunk protocol type. ▪ [1] = Shutting down (read only). ▪ [2] = Unlock the trunk (default); enables trunk traffic. <p>Notes:</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ When the device is locked from the Web interface, this parameter changes to 0. ▪ To define the administrative state per trunk, use the TrunkAdministrativeState parameter.
[TrunkAdministrativeState_x]	<p>Defines the administrative state per trunk, where x depicts the trunk number.</p> <ul style="list-style-type: none"> ▪ [0] = Lock the trunk; stops trunk traffic to configure the trunk protocol type. ▪ [1] = shutting down (read only). ▪ [2] = Unlock the trunk (default); enables trunk traffic.
Web/EMS: Line Build Out Loss [LineBuildOut.Loss]	<p>Defines the line build out loss for the selected T1 trunk.</p> <ul style="list-style-type: none"> ▪ [0] 0 dB (default) ▪ [1] -7.5 dB ▪ [2] -15 dB ▪ [3] -22.5 dB <p>Note: This parameter is applicable only to T1 trunks.</p>
[TDMHairPinning]	<p>Defines static TDM hair-pinning (cross-connection) performed at initialization. The connection is between trunks with an option to exclude a single B-Channel in each trunk. Format example: T0-T1/B3,T2-T3,T4-T5/B2.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: Enable TDM Tunneling EMS: TDM Over IP [EnableTDMoverIP]	<p>Enables TDM tunneling.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default). ▪ [1] Enable = TDM Tunneling is enabled. <p>When TDM Tunneling is enabled, the originating device automatically initiates SIP calls from all enabled B-channels pertaining to E1/T1/J1 spans that are configured with the 'Transparent' protocol. The called number of each call is the internal phone number of the B-channel from where the call originates. The 'The Inbound IP Routing Table is used to define the destination IP address of the terminating device. The terminating device automatically answers these calls if its E1/T1 protocol is set to 'Transparent' (ProtocolType = 5).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ For an overview on TDM tunneling, see 'TDM Tunneling' on page 236.

A.12.6.2 TDM Bus and Clock Timing Parameters

The TDM Bus parameters are described in the table below.

Table A-56: TDM Bus and Clock Timing Parameters

Parameter	Description
TDM Bus Parameters	
Web/EMS: PCM Law Select [PCMLawSelect]	<p>Determines the type of pulse-code modulation (PCM) companding algorithm law in input and output TDM bus.</p> <ul style="list-style-type: none"> ▪ [1] Alaw = A-law ▪ [3] MuLaw = Mu-Law <p>The default value is automatically selected according to the Protocol Type of the selected trunk: E1 defaults to ALaw, T1 defaults to MuLaw. If the Protocol Type is set to NONE, the default is MuLaw.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ Typically, A-Law is used for E1 spans and Mu-Law for T1/J1 spans.
Web/EMS: Idle PCM Pattern [IdlePCMPattern]	<p>Defines the PCM Pattern that is applied to the E1/T1 timeslot (B-channel) when the channel is idle.</p> <p>The range is 0 to 255. The default is set internally according to the Law select 1 (0xFF for Mu-Law; 0x55 for A-law).</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web/EMS: Idle ABCD Pattern [IdleABCDPattern]	<p>Defines the ABCD (CAS) Pattern that is applied to the CAS signaling bus when the channel is idle.</p> <p>The valid range is 0x0 to 0xF. The default is -1 (i.e., default pattern is 0000).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is applicable only when using PSTN interface with CAS protocols.
Web/EMS: TDM Bus Clock Source [TDMBusClockSource]	<p>Determines the clock source to which the device synchronizes.</p> <ul style="list-style-type: none"> ▪ [1] Internal = Generate clock from local source (default). ▪ [4] Network = Recover clock from PSTN line.
EMS/Web: TDM Bus Local Reference [TDMBusLocalReference]	<p>Defines the physical Trunk ID from which the device recovers (receives) its clock synchronization.</p> <p>The range is 0 to the maximum number of Trunks. The default is 0.</p> <p>Note: This parameter is applicable only if the parameter TDMBusClockSource is set to 4 and the parameter TDMBusPSTNAutoClockEnable is set to 0.</p>
Web/EMS: TDM Bus Enable Fallback [TDMBusEnableFallback]	<p>Defines the automatic fallback of the clock.</p> <ul style="list-style-type: none"> ▪ [0] Manual (default) ▪ [1] Auto Non-Revertive ▪ [2] Auto Revertive

Parameter	Description
Web: TDM Bus Fallback Clock Source EMS: TDM Bus Fallback Clock [TDMBusFallbackClock]	Determines the fallback clock source on which the device synchronizes in the event of a clock failure. <ul style="list-style-type: none"> ▪ [4] Network (default) ▪ [8] H.110_A ▪ [9] H.110_B ▪ [10] NetReference1 ▪ [11] NetReference2
Web/EMS: TDM Bus Net Reference Speed [TDMBusNetrefSpeed]	Defines the NetRef frequency (for both generation and synchronization). <ul style="list-style-type: none"> ▪ [0] 8 kHz (default) ▪ [1] 1.544 MHz ▪ [2] 2.048 MHz
Web: TDM Bus PSTN Auto FallBack Clock EMS: TDM Bus Auto Fall Back Enable [TDMBusPSTNAutoClockEnable]	Enables the PSTN trunk Auto-Fallback Clock feature. <ul style="list-style-type: none"> ▪ [0] Disable (default) = Recovers the clock from the E1/T1 line defined by the parameter TDMBusLocalReference. ▪ [1] Enable = Recovers the clock from any connected synchronized slave E1/T1 line. If this trunk loses its synchronization, the device attempts to recover the clock from the next trunk. Note that initially, the device attempts to recover the clock from the trunk defined by the parameter TDMBusLocalReference. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is relevant only if the parameter TDMBusClockSource is set to 4.
Web: TDM Bus PSTN Auto Clock Reverting EMS: TDM Bus Auto Fall Back Reverting Enable [TDMBusPSTNAutoClockRevertingEnable]	Enables the PSTN trunk Auto-Fallback Reverting feature. If enabled and a trunk returning to service has an AutoClockTrunkPriority parameter value that is higher than the priority of the local reference trunk (set in the TDMBusLocalReference parameter), the local reference reverts to the trunk with the higher priority that has returned to service for the device's clock source. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is applicable only when the TDMBusPSTNAutoClockEnable parameter is set to 1.
Web: Auto Clock Trunk Priority EMS: Auto Trunk Priority [AutoClockTrunkPriority]	Defines the trunk priority for auto-clock fallback (per trunk parameter). <ul style="list-style-type: none"> ▪ 0 to 99 = priority, where 0 (default) is the highest. ▪ 100 = the SW never performs a fallback to that trunk (usually used to mark untrusted source of clock). <p>Note: Fallback is enabled when the TDMBusPSTNAutoClockEnable parameter is set to 1.</p>

A.12.6.3 CAS Parameters

The Common Channel Associated (CAS) parameters are described in the table below. Note that CAS is not applicable to BRI interfaces.

Table A-57: CAS Parameters

Parameter	Description
Web: CAS Transport Type EMS: CAS Relay Transport Mode [CASTransportType]	<p>Determines the ABCD signaling transport type over IP.</p> <ul style="list-style-type: none"> ▪ [0] CAS Events Only = Disable CAS relay (default). ▪ [1] CAS RFC2833 Relay = Enable CAS relay mode using RFC 2833. <p>The CAS relay mode can be used with the TDM tunneling feature to enable tunneling over IP for both voice and CAS signaling bearers.</p>
[CASAddressingDelimiters]	<p>Enables the addition of delimiters to the received address or received ANI digits string.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default). The address and ANI strings remain without delimiters. ▪ [1] = Enable. Delimiters such as '*', '#', and 'ST' are added to the received address or received ANI digits string.
[CASDelimitersPaddingUsage]	<p>Defines the digits string delimiter padding usage per trunk.</p> <ul style="list-style-type: none"> ▪ [0] (default) = default address string padding: '*XXX#' (where XXX is the digit string that begins with '*' and ends with '#', when using padding). ▪ [1] = special use of asterisks delimiters: '*XXX*YYY*' (where XXX is the address, YYY is the source phone number, and '*' is the only delimiter padding). <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: CAS Table per Trunk EMS: Trunk CAS Table Index [CASTableIndex_x]	<p>Defines the CAS protocol per trunk (where x denotes the trunk ID) from a list of CAS protocols defined by the parameter CASFileName_x.</p> <p>For example, the below configuration specifies Trunks 0 and 1 to use the E&M Winkstart CAS (E_M_WinkTable.dat) protocol, and Trunks 2 and 3 to use the E&M Immediate Start CAS (E_M_ImmediateTable.dat) protocol:</p> <pre>CASFileName_0 = 'E_M_WinkTable.dat' CASFileName_1 = 'E_M_ImmediateTable.dat' CASTableIndex_0 = 0 CASTableIndex_1 = 0 CASTableIndex_2 = 1 CASTableIndex_3 = 1</pre> <p>Note: You can define CAS tables per B-channel using the parameter CASChannelIndex.</p>
Web: Dial Plan EMS: Dial Plan Name [CASTrunkDialPlanName_x]	<p>Defines the CAS Dial Plan name that is used on a specific trunk (where x denotes the trunk ID). The range is up to 11 characters.</p> <p>For example, the below configures E1_MFCR2 trunk with a single protocol (Trunk 5):</p> <pre>ProtocolType_5 = 7 CASFileName_0='R2_Korea_CP_ANI.dat' CASTableIndex_5 = 0</pre>

Parameter	Description
	DialPlanFileName = 'DialPlan_USA.dat' CASTrunkDialPlanName_5 = 'AT_T'
[CASFileName_x]	Defines the CAS file name (e.g., 'E_M_WinkTable.dat') that defines the CAS protocol, where x denotes the CAS file ID (0-7). It is possible to define up to eight different CAS files by repeating this parameter. Each CAS file can be associated with one or more of the device's trunks, using the parameter CASTableIndex_x. Note: For this parameter to take effect, a device reset is required.
Web: CAS Table per Channel [CASChannelIndex]	Defines the loaded CAS protocol table index per B-channel pertaining to a CAS trunk. This parameter is assigned a string value and can be set in one of the following two formats: <ul style="list-style-type: none"> CAS table per channel: Each channel is separated by a comma and the value entered depicts the CAS table index used for that channel. The syntax is <CAS index>,<CAS index> (e.g., "1,2,1,2..."). For this format, 31 indices must be defined for E1 trunks (including dummy for B-channel 16), or 24 indices for T1 trunks. Below is an example for configuring a T1 CAS trunk (Trunk 5) with several CAS variants <pre data-bbox="614 862 1388 1097"> ProtocolType_5 = 7 CASFILENAME_0='E_M_FGBWinkTable.dat' CASFILENAME_1='E_M_FGDWinkTable.dat' CASFILENAME_2='E_M_WinkTable.txt' CasChannelIndex_5 = `0,0,0,1,1,1,2,2,2,0,0,0,1,1,1,0,1,2,0,2,1,2,2, 2' CASDelimitersPaddingUsage_5 = 1 </pre> CAS table per channel group: Each channel group is separated by a colon and each channel is separated by a comma. The syntax is <x-y channel range>:<CAS table index>, (e.g., "1-10:1,11-31:3"). Every B-channel (including 16 for E1) must belong to a channel group. Below is an example for configuring an E1 CAS trunk (Trunk 5) with several CAS variants: <pre data-bbox="614 1332 1388 1444"> ProtocolType_5 = 8 CASFILENAME_2='E1_R2D' CASFILENAME_7='E_M_ImmediateTable_A-Bit.txt' CasChannelIndex_5 = `1-10:2,11-20:7,21-31:2' </pre> Notes: <ul style="list-style-type: none"> To configure this parameter, the trunk must first be stopped. Only one of these formats can be implemented; not both. When this parameter is not configured, a single CAS table for the entire trunk is used, configured by the parameter CASTableIndex.
[CASTablesNum]	Defines how many CAS protocol configurations files are loaded. The valid range is 1 to 8. Note: For this parameter to take effect, a device reset is required.
CAS State Machines Parameters Note: For configuring the CAS State Machine table using the Web interface, see 'Configuring CAS State Machines' on page 229 .	
Web: Generate Digit On Time [CASStateMachineGenerateDigitOnTime]	Generates digit on-time (in msec). The value must be a positive value. The default value is -1.

Parameter	Description
Web: Generate Inter Digit Time [CASStateMachineGenerateInterDigitTime]	Generates digit off-time (in msec). The value must be a positive value. The default value is -1.
Web: DTMF Max Detection Time [CASStateMachineDTMFMaxOnDetectionTime]	Detects digit maximum on time (according to DSP detection information event) in msec units. The value must be a positive value. The default value is -1.
Web: DTMF Min Detection Time [CASStateMachineDTMFMinOnDetectionTime]	Detects digit minimum on time (according to DSP detection information event) in msec units. The digit time length must be longer than this value to receive a detection. Any number may be used, but the value must be less than CasStateMachineDTMFMaxOnDetectionTime. The value must be a positive value. The default value is -1.
Web: MAX Incoming Address Digits [CASStateMachineMaxNumOfIncomingAddressDigits]	Defines the limitation for the maximum address digits that need to be collected. After reaching this number of digits, the collection of address digits is stopped. The value must be an integer. The default value is -1.
Web: MAX Incoming ANI Digits [CASStateMachineMaxNumOfIncomingANIDigits]	Defines the limitation for the maximum ANI digits that need to be collected. After reaching this number of digits, the collection of ANI digits is stopped. The value must be an integer. The default value is -1.
Web: Collect ANI [CASStateMachineCollectANI]	In some cases, when the state machine handles the ANI collection (not related to MFCR2), you can enable the state machine to collect ANI or discard ANI. <ul style="list-style-type: none"> ▪ [0] No = Don't collect ANI. ▪ [1] Yes = Collect ANI. ▪ [-1] Default = Default value.
Web: Digit Signaling System [CASStateMachineDigitSignalingSystem]	Defines which Signaling System to use in both directions (detection\generation). <ul style="list-style-type: none"> ▪ [0] DTMF = Uses DTMF signaling. ▪ [1] MF = Uses MF signaling (default). ▪ [-1] Default = Default value.

A.12.6.4 ISDN Parameters

The ISDN parameters are described in the table below.

Table A-58: ISDN Parameters

Parameter	Description
Web: ISDN Termination Side EMS: Termination Side [TerminationSide]	Determines the ISDN termination side. <ul style="list-style-type: none"> ▪ [0] User side = ISDN User Termination Equipment (TE) side (default) ▪ [1] Network side = ISDN Network Termination (NT) side <p>Note: Select 'User side' when the PSTN or PBX side is configured as 'Network side' and vice versa. If you don't know the device's ISDN termination side, choose 'User side'. If the D-channel alarm is indicated, choose 'Network Side'.</p> <p>The BRI module supports the ITU-T I.430 standard, which defines the ISDN-BRI layer 1 specification. The BRI and PRI ports are configured similarly, using this parameter. When an NT port is active, it drives a 38-V line and sends an INFO1 signal (as defined in ITU-T I.430 Table 4) on the data line to synchronize to a TE port that might be connected to it. To stop the voltage and the INFO1 signal on the line, stop the trunk using the Stop Trunk button.</p>
[TerminationSide_x]	Same as the description for parameter TerminationSide, but for a specific trunk ID (where x denotes the Trunk ID and 0 is the first Trunk).
BRI Layer 2 Mode [BriLayer2Mode]	Determines whether Point-to-Point or Point-to-Multipoint mode for BRI ports. <ul style="list-style-type: none"> ▪ [0] Point to Point (default) ▪ [1] Point to Multipoint = Must be configured for Network side.
Web/EMS: B-channel Negotiation [BchannelNegotiation]	Determines the ISDN B-Channel negotiation mode. <ul style="list-style-type: none"> ▪ [0] Preferred. ▪ [1] Exclusive (default). ▪ [2] Any. <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only to ISDN protocols. ▪ For some ISDN variants, when 'Any' (2) is selected, the Setup message excludes the Channel Identification IE. ▪ The 'Any' (2) option is applicable only if the following conditions are met: <ul style="list-style-type: none"> ✓ The parameter TerminationSide is set to 0 ('User side'). ✓ The PSTN protocol type (ProtocolType) is configured as Euro ISDN.
NFAS Parameters Note: These parameters are applicable to PRI interfaces.	
Web: NFAS Group Number EMS: Group Number [NFASGroupNumber_x]	Defines the NFAS group number (NFAS member) for the selected trunk, where x depicts the Trunk ID. <ul style="list-style-type: none"> ▪ 0 = Non-NFAS trunk (default) ▪ 1 to 12 = NFAS group number <p>Trunks that belong to the same NFAS group have the same number.</p> <p>With ISDN Non-Facility Associated Signaling you can use single</p>

Parameter	Description
	<p>D-channel to control multiple PRI interfaces.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is applicable only to T1 ISDN protocols. ▪ For more information on NFAS, see 'ISDN Non-Facility Associated Signaling (NFAS)' on page 246.
<p>Web/EMS: D-channel Configuration [DChConfig_x]</p>	<p>Defines primary, backup (optional), and B-channels only, per trunk (where x depicts the Trunk ID).</p> <ul style="list-style-type: none"> ▪ [0] PRIMARY= Primary Trunk (default) - contains a D-channel that is used for signaling. ▪ [1] BACKUP = Backup Trunk - contains a backup D-channel that is used if the primary D-channel fails. ▪ [2] NFAS = NFAS Trunk - contains only 24 B-channels, without a signaling D-channel. <p>Note: This parameter is applicable only to T1 ISDN protocols.</p>
<p>Web: NFAS Interface ID EMS: ISDN NFAS Interface ID [ISDNNFASInterfaceID_x]</p>	<p>Defines a different Interface ID for each T1 trunk (where x denotes the trunk ID). The valid range is 0 to 100. The default interface ID equals the trunk's ID.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ To set the NFAS interface ID, configure ISDNIBehavior_x to include '512' feature per T1 trunk. ▪ For more information on NFAS, see 'ISDN Non-Facility Associated Signaling (NFAS)' on page 246.
<p>Web: Enable ignoring ISDN Disconnect with PI [KeepISDNCallOnDisconnectWithPI]</p>	<p>Allows the device to ignore ISDN Disconnect messages with PI 1 or 8.</p> <ul style="list-style-type: none"> ▪ [1] = The call (in connected state) is not released if a Q.931 Disconnect with PI (PI = 1 or 8) message is received during the call. ▪ [0] = The call is disconnected (default).
<p>Web: PI For Setup Message [PIForSetupMsg]</p>	<p>Determines whether and which Progress Indicator (PI) information element (IE) is added to the sent ISDN Setup message. Some ISDN protocols such as NI-2 or Euro ISDN can optionally contain PI = 1 or PI = 3 in the Setup message.</p> <ul style="list-style-type: none"> ▪ [0] = PI is not added (default). ▪ [1] = PI 1 is added to a sent ISDN Setup message - call is not end-to-end ISDN. ▪ [3] = PI 3 is added to a sent ISDN Setup message - calling equipment is not ISDN.
<p>ISDN Flexible Behavior Parameters ISDN protocol is implemented in different switches/PBXs by different vendors. Several implementations may vary slightly from the specification. Therefore, to provide a flexible interface that supports these ISDN variants, the ISDN behavior parameters can be used.</p>	
<p>Web/EMS: Incoming Calls Behavior [ISDNInCallsBehavior]</p>	<p>Determines the bit-field used to determine several behavior options that influence how the ISDN Stack INCOMING calls behave.</p> <ul style="list-style-type: none"> ▪ [32] DATA CONN RS = The device sends a Connect (answer) message on not incoming Tel calls. ▪ [64] VOICE CONN RS = The device sends a Connect

Parameter	Description
	<p>(answer) message on incoming Tel calls.</p> <ul style="list-style-type: none"> ▪ [2048] CHAN ID IN FIRST RS = The device sends Channel ID in the first response to an incoming Q.931 Call Setup message. Otherwise, the Channel ID is sent only if the device requires changing the proposed Channel ID (default). ▪ [8192] CHAN ID IN CALL PROC = The device sends Channel ID in a Q.931 Call Proceeding message. ▪ [65536] PROGR IND IN SETUP ACK = The device includes Progress Indicator (PI=8) in Setup ACK message if an empty called number is received in an incoming Setup message. This option is applicable to the overlap dialing mode. The device also plays a dial tone (for TimeForDialTone) until the next called number digits are received. ▪ [262144] = NI-2 second redirect number. You can select and use (in INVITE messages) the NI-2 second redirect number if two redirect numbers are received in Q.931 Setup for incoming Tel-to-IP calls. ▪ [2147483648] CC_USER_SCREEN_INDICATOR = When the device receives two Calling Number IE's in the Setup message, the device by default, uses only one of the numbers according to the following: <ul style="list-style-type: none"> ✓ Network provided, Network provided - the first calling number is used ✓ Network provided, User provided: the first one is used ✓ User provided, Network provided: the second one is used ✓ User provided, user provided: the first one is used <p>When this bit is configured, the device behaves as follows:</p> <ul style="list-style-type: none"> ✓ Network provided, Network provided: the first calling number is used ✓ Network provided, User provided: the second one is used ✓ User provided, Network provided: the first one is used ✓ User provided, user provided: the first one is used <p>Note: When using the <i>ini</i> file to configure the device to support several ISDNInCallsBehavior features, enter a summation of the individual feature values. For example, to support both [2048] and [65536] features, set ISDNInCallsBehavior = 67584 (i.e., 2048 + 65536).</p>
[ISDNInCallsBehavior_x]	Same as the description for the parameter ISDNInCallsBehavior, but per trunk (i.e., where x depicts the Trunk ID).
Web/EMS: Q.931 Layer Response Behavior [ISDNIBehavior]	<p>Bit-field used to determine several behavior options that influence the behaviour of the Q.931 protocol.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] NO STATUS ON UNKNOWN IE = Q.931 Status message isn't sent if Q.931 received message contains an unknown/unrecognized IE. By default, the Status message is sent. Note: This value is applicable only to ISDN variants in which sending of Status message is optional. ▪ [2] NO STATUS ON INV OP IE = Q.931 Status message isn't sent if an optional IE with invalid content is received. By default, the Status message is sent. Note: This option is applicable only to ISDN variants in which sending of Status message is optional. ▪ [4] ACCEPT UNKNOWN FAC IE = Accepts

Parameter	Description
	<p>unknown/unrecognized Facility IE. Otherwise, the Q.931 message that contains the unknown Facility IE is rejected (default).</p> <p>Note: This option is applicable only to ISDN variants where a complete ASN1 decoding is performed on Facility IE.</p> <ul style="list-style-type: none"> ▪ [128] SEND USER CONNECT ACK = The Connect ACK message is sent in response to received Q.931 Connect; otherwise, the Connect ACK is not sent (default). Note: This option is applicable only to Euro ISDN User side outgoing calls. ▪ [512] EXPLICIT INTERFACE ID = Enables to configure T1 NFAS Interface ID (refer to the parameter ISDNNFASInterfaceID_x). Note: This value is applicable only to 4/5ESS, DMS, NI-2 and HKT variants. ▪ [2048] ALWAYS EXPLICIT = Always set the Channel Identification IE to explicit Interface ID, even if the B-channel is on the same trunk as the D-channel. Note: This value is applicable only to 4/5ESS, DMS and NI-2 variants. ▪ [32768] ACCEPT MU LAW =Mu-Law is also accepted in ETSI. ▪ [65536] EXPLICIT PRES SCREENING = The calling party number (octet 3a) is always present even when presentation and screening are at their default. Note: This option is applicable only to ETSI, NI-2, and 5ESS. ▪ [131072] STATUS INCOMPATIBLE STATE = Clears the call on receipt of Q.931 Status with incompatible state. Otherwise, no action is taken (default). ▪ [262144] STATUS ERROR CAUSE = Clear call on receipt of Status according to cause value. ▪ [524288] ACCEPT A LAW =A-Law is also accepted in 5ESS. ▪ [2097152] RESTART INDICATION = Upon receipt of a Restart message, acEV_PSTN_RESTART_CONFIRM is generated. ▪ [4194304] FORCED RESTART = On data link (re)initialization, send RESTART if there is no call. ▪ [67108864] NS ACCEPT ANY CAUSE = Accept any Q.850 Cause IE from ISDN. Note: This option is applicable only to Euro ISDN. ▪ [134217728] NS_BRI_DL_ALWAYS_UP (0x08000000) = By default, the BRI D-channel goes down if there are no active calls. If this option is configured, the BRI D-channel is always up and synchronized. ▪ [536870912] Alcatel coding for redirect number and display name is accepted by the device. Note: This option is applicable only to QSIG (and relevant for specific Alcatel PBXs such as OXE). ▪ [1073741824] QSI ENCODE INTEGER = If this bit is set, INTEGER ASN.1 type is used in operator coding (compliant to new ECMA standards); otherwise, OBJECT IDENTIFIER ASN.1 type is used. Note: This option is applicable only to QSIG. ▪ [2147483648] 5ESS National Mode For Bch Maintenance =

Parameter	Description
	Use the National mode of AT&T 5ESS for B-channel maintenance. Notes: <ul style="list-style-type: none"> ▪ To configure the device to support several ISDNBehavior features, enter a summation of the individual feature values. For example, to support both [512] and [2048] features, set the parameter ISDNBehavior is set to 2560 (i.e., 512 + 2048). ▪ When configuring in the Web interface, to select the options click the arrow button and then for each required option select 1 to enable.
[ISDNBehavior_x]	Same as the description for parameter ISDNBehavior, but for a specific trunk ID.
Web: General Call Control Behavior EMS: General CC Behavior [ISDNGeneralCCBehavior]	Bit-field for determining several general CC behavior options. To select the options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable). <ul style="list-style-type: none"> ▪ [2] = Data calls with interworking indication use 64 kbps B-channels (physical only). ▪ [8] REVERSE CHAN ALLOC ALGO = Channel ID allocation algorithm. ▪ [16] = The device clears down the call if it receives a NOTIFY message specifying 'User-Suspended'. A NOTIFY (User-Suspended) message is used by some networks (e.g., in Italy or Denmark) to indicate that the remote user has cleared the call, especially in the case of a long distance voice call. ▪ [32] CHAN ID 16 ALLOWED = Applies only to ETSI E1 lines (30B+D). Enables handling the differences between the newer QSIG standard (ETS 300-172) and other ETSI-based standards (ETS 300-102 and ETS 300-403) in the conversion of B-channel ID values into timeslot values: <ul style="list-style-type: none"> ✓ In 'regular ETSI' standards, the timeslot is identical to the B-channel ID value, and the range for both is 1 to 15 and 17 to 31. The D-channel is identified as channel-id #16 and carried into the timeslot #16. ✓ In newer QSIG standards, the channel-id range is 1 to 30, but the timeslot range is still 1 to 15 and 17 to 31. The D-channel is not identified as channel-id #16, but is still carried into the timeslot #16. When this bit is set, the channel ID #16 is considered as a valid B-channel ID, but timeslot values are converted to reflect the range 1 to 15 and 17 to 31. This is the new QSIG mode of operation. When this bit is not set (default), the channel_id #16 is not allowed, as for all ETSI-like standards. ▪ [64] USE T1 PRI = PRI interface type is forced to T1. ▪ [128] USE E1 PRI = PRI interface type is forced to E1. ▪ [256] START WITH B CHAN OOS = B-channels start in the Out-Of-Service state (OOS). ▪ [512] CHAN ALLOC LOWEST = CC allocates B-channels starting from the lowest available B-channel id. ▪ [1024] CHAN ALLOC HIGHEST = CC allocates B-channels starting from the highest available B-channel id. ▪ [16384] CC_TRANSPARENT_UUI bit: The UUI-protocol implementation of CC is disabled allowing the application to freely send UUI elements in any primitive, regardless of the

Parameter	Description
	<p>UUI-protocol requirements (UUI Implicit Service 1). This allows more flexible application control on the UUI. When this bit is not set (default behavior), CC implements the UUI-protocol as specified in the ETS 300-403 standards for Implicit Service 1.</p> <ul style="list-style-type: none"> ▪ [65536] GTD5 TBCT = CC implements the VERIZON-GTD-5 Switch variant of the TBCT Supplementary Service, as specified in FSD 01-02-40AG Feature Specification Document from Verizon. Otherwise, TBCT is implemented as specified in GR-2865-CORE specification (default behavior). <p>Note: When using the <i>ini</i> file to configure the device to support several ISDNGeneralCCBehavior features, add the individual feature values. For example, to support both [16] and [32] features, set ISDNGeneralCCBehavior = 48 (i.e., 16 + 32).</p>
<p>Web/EMS: Outgoing Calls Behavior [ISDNOutCallsBehavior]</p>	<p>Determines several behaviour options (bit fields) that influence the behaviour of the ISDN Stack outgoing calls. To select options, click the arrow button, and then for each required option, select 1 to enable. The default is 0 (i.e., disable).</p> <ul style="list-style-type: none"> ▪ [2] USER SENDING COMPLETE = The device doesn't automatically generate the Sending-Complete IE in the Setup message. If this bit is not set, the device generates it automatically in the Setup message only. ▪ [16] USE MU LAW = The device sends G.711-m-Law in outgoing voice calls. When disabled, the device sends G.711-A-Law in outgoing voice calls. Note: This option is applicable only to the Korean variant. ▪ [128] DIAL WITH KEYPAD = The device uses the Keypad IE to store the called number digits instead of the CALLED_NB IE. Note: This option is applicable only to the Korean variant (Korean network). This is useful for Korean switches that don't accept the CALLED_NB IE. ▪ [256] STORE CHAN ID IN SETUP = The device forces the sending of a Channel-Id IE in an outgoing Setup message even if it's not required by the standard (i.e., optional) and no Channel-Id has been specified in the establishment request. This is useful for improving required compatibility with switches. On BRI lines, the Channel-Id IE indicates 'any channel'. On PRI lines, it indicates an unused channel ID, preferred only. ▪ [572] USE A LAW = The device sends G.711 A-Law in outgoing voice calls. When disabled, the device sends the default G.711-Law in outgoing voice calls. Note: This option is applicable only to the E10 variant. ▪ [1024] = Numbering plan/type for T1 IP-to-Tel calling numbers are defined according to the manipulation tables or according to the RPID header (default). Otherwise, the plan/type for T1 calls are set according to the length of the calling number. ▪ [2048] = The device accepts any IA5 character in the called_nb and calling_nb strings and sends any IA5 character in the called_nb, and is not restricted to extended digits only (i.e., 0-9,*,#). ▪ [16384] DLCI REVERSED OPTION = Behavior bit used in the IUA interface groups to indicate that the reversed format of the DLCI field must be used.

Parameter	Description
	<p>Note: When using the <i>ini</i> file to configure the device to support several ISDNOutCallsBehavior features, add the individual feature values. For example, to support both [2] and [16] features, set ISDNOutCallsBehavior = 18 (i.e., 2 + 16).</p>
[ISDNOutCallsBehavior_x]	Same as the description for parameter ISDNOutCallsBehavior, but for a specific trunk ID.
Web: ISDN NS Behaviour 2 [ISDNNSBehaviour2]	<p>Bit-field to determine several behavior options that influence the behavior of the Q.931 protocol.</p> <ul style="list-style-type: none"> ▪ [8] NS_BEHAVIOUR2_ANY_UUI: any User to User Information Element (UUIE) is accepted for any protocol discriminator. This is useful for interoperability with non-standard switches.
[PSTNExtendedParams]	<p>Determines the bit map for special PSTN behavior parameters:</p> <ul style="list-style-type: none"> ▪ [0] (default) = For QSIG "Networking Extensions". This bit (bit #0) is responsible for the Invokeld size: <ul style="list-style-type: none"> ✓ If this bit is not set (default), then the Invokeld size is one byte. ✓ If this bit is set, then the Invokeld size is two bytes. ▪ [2] = For ROSE format (according to old QSIG specifications). This bit (bit #1) is responsible for the QSIG octet 3. According to the ECMA-165 new version, octet 3 in all QSIG supplementary services Facility messages should be 0x9F = Networking Extensions. However, according to the old version, the value should be 0x91 = ROSE: <ul style="list-style-type: none"> ✓ If this bit is not set (default): 0x9F = Networking Extensions ✓ If this bit is set: 0x91 = ROSE <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ If you want to use both the above options, then set this parameter to 3.

A.12.7 ISDN and CAS Interworking Parameters

The ISDN and CAS interworking parameters are described in the table below.

Table A-59: ISDN and CAS Interworking Parameters

Parameter	Description
ISDN Parameters	
Web: Send Local Time To ISDN Connect [SendLocalTimeToISDNConnect]	<p>Enables the device to send the date and time in the ISDN Connect message (Date / Time Information Element) if the received SIP 200 OK message is received without the SIP Date header. The device obtains the date and time from its internal clock. This feature is applicable only to Tel-to-IP calls.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) = If the SIP 200 OK contains the Date header, the device sends its value in the ISDN Connect Date / Time IE. If the 200 OK does not include this header, it does not add the Date / Time IE to the sent ISDN Connect message.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [1] Enable = If the SIP 200 OK contains the Date header, the device sends its value (i.e. date and time) in the ISDN Connect Date / Time IE. If the 200 OK does not include this header, the device uses its internal, local date and time for the Date / Time IE, which it adds to the sent ISDN Connect message. <p>Note: For IP-to-Tel calls, this parameter is not applicable. Only if the incoming ISDN Connect message contains the Date / Time IE does the device add the Date header to the sent SIP 200 OK message.</p>
Web/EMS: Min Routing Overlap Digits [MinOverlapDigitsForRouting]	Defines the minimum number of overlap digits to collect (for ISDN overlap dialing) before sending the first SIP message for routing Tel-to-IP calls. The valid value range is 0 to 49. The default is 1. <p>Note: This parameter is applicable when the ISDNRxOverlap parameter is set to [2].</p>
Web/EMS: ISDN Overlap IP to Tel Dialing [ISDNTxOverlap]	Enables ISDN overlap dialing for IP-to-Tel calls. This feature is part of ISDN-to-SIP overlap dialing according to RFC 3578. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable When enabled, for each received INVITE of the same dialog session, the device sends an ISDN Setup (and subsequent ISDN Info Q.931 messages) with the collected digits to the Tel side. For all subsequent INVITEs received, the device sends a SIP 484 Address Incomplete response in order to maintain the current dialog session and receive additional digits from subsequent INVITEs. <p>Note: When IP-to-Tel overlap dialing is enabled, to send ISDN Setup messages without the Sending Complete IE, the ISDNOutCallsBehavior parameter must be set to USER SENDING COMPLETE (2).</p>
Web: Enable Receiving of Overlap Dialing [ISDNRxOverlap_x]	Determines the receiving (Rx) type of ISDN overlap dialing for Tel-to-IP calls. <ul style="list-style-type: none"> ▪ [0] None (default) = Disabled. ▪ [1] Local receiving = ISDN Overlap Dialing - the complete number is sent in the INVITE Request-URI user part. The device receives ISDN called number that is sent in the 'Overlap' mode. The ISDN Setup message is sent to IP only after the number (including the Sending Complete IE) is fully received (via Setup and/or subsequent Info Q.931 messages). In other words, the device waits until it has received all the ISDN signaling messages containing parts of the called number, and only then it sends a SIP INVITE with the entire called number in the Request-URI. ▪ [2] Through SIP = Interworking of ISDN Overlap Dialing to SIP, based on RFC 3578. The device interworks ISDN to SIP by sending digits each time they are received (from Setup and subsequent Info Q.931 messages) to the IP, using subsequent SIP INVITE messages. <p>Notes:</p> <ul style="list-style-type: none"> ▪ When option [2] is configured, you can define the minimum number of overlap digits to collect before sending the first

Parameter	Description
	<p>SIP message for routing the call, using the MinOverlapDigitsForRouting parameter.</p> <ul style="list-style-type: none"> ▪ When option [2] is configured, even if SIP 4xx responses are received during this ISDN overlap receiving, the device does not release the call. ▪ The MaxDigits parameter can be used to limit the length of the collected number for ISDN overlap dialing (if Sending Complete is not received). ▪ If a digit map pattern is defined (using the DigitMapping or DialPlanIndex parameters), the device collects digits until a match is found (e.g., for closed numbering schemes) or until a timer expires (e.g., for open numbering schemes). If a match is found (or the timer expires), the digit collection process is terminated even if Sending Complete is not received. ▪ For enabling ISDN overlap dialing for IP-to-Tel calls, use the ISDNTxOverlap parameter. ▪ For more information on ISDN overlap dialing, see 'ISDN Overlap Dialing' on page 244.
[ISDNRxOverlap]	Same as the description for parameter ISDNRxOverlap_x, but for all trunks.
Web/EMS: Mute DTMF In Overlap [MuteDTMFInOverlap]	<p>Enables the muting of in-band DTMF detection until the device receives the complete destination number from the ISDN (for Tel-to-IP calls). In other words, the device does not accept DTMF digits received in the voice stream from the PSTN, but only accepts digits from ISDN Info messages.</p> <ul style="list-style-type: none"> ▪ [0] Don't Mute (default) ▪ [1] Mute DTMF in Overlap Dialing = The device ignores in-band DTMF digits received during ISDN overlap dialing (disables the DTMF in-band detector). <p>Note: This parameter is applicable to ISDN Overlap mode only when dialed numbers are sent using Q.931 Information messages.</p>
[ConnectedNumberType]	<p>Defines the Numbering Type of the ISDN Q.931 Connected Number IE that the device sends in the Connect message to the ISDN (for Tel-to-IP calls). This is interworked from the P-Asserted-Identity header in SIP 200 OK.</p> <p>The default is [0] (i.e., unknown).</p>
[ConnectedNumberPlan]	<p>Defines the Numbering Plan of the ISDN Q.931 Connected Number IE that the device sends in the Connect message to the ISDN (for Tel-to-IP calls). This is interworked from the P-Asserted-Identity header in SIP 200 OK.</p> <p>The default is [0] (i.e., unknown).</p>
Web/EMS: Enable ISDN Tunneling Tel to IP [EnableISDNTunnelingTel2IP]	<p>Enables ISDN Tunneling.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default). ▪ [1] Using Header = Enable ISDN Tunneling from ISDN PRI to SIP using a proprietary SIP header. ▪ [2] Using Body = Enable ISDN Tunneling from ISDN PRI to SIP using a dedicated message body. <p>When ISDN Tunneling is enabled, the device sends all ISDN PRI messages using the correlated SIP messages. The ISDN</p>

Parameter	Description
	<p>Setup message is tunneled using SIP INVITE, all mid-call messages are tunneled using SIP INFO, and ISDN Disconnect/Release message is tunneled using SIP BYE messages. The raw data from the ISDN is inserted into a proprietary SIP header (X-ISDNTunnelingInfo) or a dedicated message body (application/isdn) in the SIP messages.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this feature to function, you must set the parameter <code>ISDNDuplicateQ931BuffMode</code> to 128 (i.e., duplicate all messages). ▪ ISDN tunneling is applicable for all ISDN variants as well as QSIG.
<p>Web/EMS: Enable ISDN Tunneling IP to Tel [EnableISDNTunnelingIP2Tel]</p>	<p>Enables ISDN Tunneling to the Tel side.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable ISDN Tunneling from IP to ISDN <p>When ISDN Tunneling is enabled, the device extracts raw data received in a proprietary SIP header (X-ISDNTunnelingInfo) or a dedicated message body (application/isdn) in the SIP messages and sends the data as ISDN messages to the PSTN side.</p>
<p>Web/EMS: Enable QSIG Tunneling [EnableQSIGTunneling]</p>	<p>Enables QSIG tunneling-over-SIP for all calls. This is according to IETF Internet-Draft draft-elwell-sipping-qsig-tunnel-03 and ECMA-355 and ETSI TS 102 345.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default). ▪ [1] Enable = Enable QSIG tunneling from QSIG to SIP and vice versa. All QSIG messages are sent as raw data in corresponding SIP messages using a dedicated message body. <p>Notes:</p> <ul style="list-style-type: none"> ▪ You can enable QSIG tunneling per specific calls by enabling QSIG tunneling for an IP Profile. ▪ QSIG tunneling must be enabled on originating and terminating devices. ▪ To enable this function, set the <code>ISDNDuplicateQ931BuffMode</code> parameter to 128 (i.e., duplicate all messages). ▪ To define the format of encapsulated QSIG messages, use the <code>QSIGTunnelingMode</code> parameter. ▪ Tunneling according to ECMA-355 is applicable to all ISDN variants (in addition to the QSIG protocol). ▪ For more information on QSIG tunneling, see 'QSIG Tunneling' on page 239.
<p>[QSIGTunnelingMode]</p>	<p>Defines the format of encapsulated QSIG message data in the SIP message MIME body.</p> <ul style="list-style-type: none"> ▪ [0] = ASCII presentation of Q.931 QSIG message (default). ▪ [1] = Binary encoding of Q.931 QSIG message (according to ECMA-355, RFC 3204, and RFC 2025). <p>Note: This parameter is applicable only if the QSIG Tunneling feature is enabled (using the <code>EnableQSIGTunneling</code> parameter).</p>

Parameter	Description
Web: Enable Hold to ISDN EMS: Enable Hold 2 ISDN [EnableHold2ISDN]	Enables SIP-to-ISDN interworking of the Hold/Retrieve supplementary service. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Notes: <ul style="list-style-type: none"> ▪ This parameter is applicable to Euro ISDN variants - from TE (user) to NT (network). ▪ This parameter is applicable also to QSIG BRI. ▪ If the parameter is disabled, the device plays a Held tone to the Tel side when a SIP request with 0.0.0.0 or "inactive" in SDP is received. An appropriate CPT file with the Held tone should be used.
EMS: Duplicate Q931 Buff Mode [ISDNDuplicateQ931BuffMode]	Determines the activation/deactivation of delivering raw Q.931 messages. <ul style="list-style-type: none"> ▪ [0] = ISDN messages aren't duplicated (default). ▪ [128] = All ISDN messages are duplicated. Note: For this parameter to take effect, a device reset is required.
Web/EMS: ISDN SubAddress Format [ISDNSubAddressFormat]	Determines the encoding format of the SIP Tel URI parameter 'isub', which carries the encoding type of ISDN subaddresses. This is used to identify different remote ISDN entities under the same phone number (ISDN Calling and Called numbers) for interworking between ISDN and SIP networks. <ul style="list-style-type: none"> ▪ [0] = ASCII - IA5 format that allows up to 20 digits. Indicates that the 'isub' parameter value needs to be encoded using ASCII characters (default) ▪ [1] = BCD (Binary Coded Decimal) - allows up to 40 characters (digits and letters). Indicates that the 'isub' parameter value needs to be encoded using BCD when translated to an ISDN message. ▪ [2] = User Specified For IP-to-Tel calls, if the incoming SIP INVITE message includes subaddress values in the 'isub' parameter for the Called Number (in the Request-URI) and/or the Calling Number (in the From header), these values are mapped to the outgoing ISDN Setup message. If the incoming ISDN Setup message includes 'subaddress' values for the Called Number and/or the Calling Number, these values are mapped to the outgoing SIP INVITE message's 'isub' parameter in accordance with RFC 4715.
[IgnoreISDNSubaddress]	Determines whether the device ignores the Subaddress from the incoming ISDN Called and Calling numbers when sending to IP. <ul style="list-style-type: none"> ▪ [0] = If an incoming ISDN Q.931 Setup message contains a Called/Calling Number Subaddress, the Subaddress is interworked to the SIP 'isub' parameter according to RFC (default). ▪ [1] = The device removes the ISDN Subaddress and does not include the 'isub' parameter in the Request-URI and does not process INVITEs with this parameter.

Parameter	Description
[ISUBNumberOfDigits]	<p>Defines the number of digits (from the end) that the device takes from the called number (received from the IP) for the isub number (in the sent ISDN Setup message). This feature is only applicable for IP-to-ISDN calls.</p> <p>The valid value range is 0 to 36. The default value is 0.</p> <p>This feature operates as follows:</p> <ol style="list-style-type: none"> 1 If an isub parameter is received in the Request-URI, for example, INVITE sip:9565645;isub=1234@host.domain:user=phone SIP/2.0 then the isub value is sent in the ISDN Setup message as the destination subaddress. 2 If the isub parameter is not received in the user part of the Request-URI, the device searches for it in the URI parameters of the To header, for example, To: "Alex" <sip: 9565645@host.domain;isub=1234> If present, the isub value is sent in the ISDN Setup message as the destination subaddress. 3 If the isub parameter is not present in the Request-URI header nor To header, the device does the following: <ul style="list-style-type: none"> ✓ If the called number (that appears in the user part of the Request-URI) starts with zero (0), for example, INVITE sip:05694564@host.domain:user=phone SIP/2.0 then the device maps this called number to the destination number of the ISDN Setup message, and the destination subaddress in this ISDN Setup message remains empty. ✓ If the called number (that appears in the user part of the Request-URI) does not start with zero, for example, INVITE sip:5694564@host.domain:user=phone SIP/2.0 then the device maps this called number to the destination number of the ISDN Setup message, and the destination subaddress in this ISDN Setup message then contains y digits from the end of the called number. The y number of digits can be configured using the ISUBNumberOfDigits parameter. The default value of ISUBNumberOfDigits is 0, thus, if this parameter is not configured, and 1) and 2) scenarios (described above) have not provided an isub value, the subaddress remains empty.
Web: Play Busy Tone to Tel [PlayBusyTone2ISDN]	<p>Enables the device to play a busy or reorder tone to the PSTN after a Tel-to-IP call is released.</p> <ul style="list-style-type: none"> ▪ [0] Don't Play = Immediately sends an ISDN Disconnect message (default). ▪ [1] Play when Disconnecting = Sends an ISDN Disconnect message with PI = 8 and plays a busy or reorder tone to the PSTN (depending on the release cause). ▪ [2] Play before Disconnect = Delays the sending of an ISDN Disconnect message for a user-defined time (configured by the TimeForReorderTone parameter) and plays a busy or reorder tone to the PSTN. This is applicable only if the call is released from the IP [Busy Here (486) or Not Found (404)] before it reaches the Connect state; otherwise, the

Parameter	Description
	Disconnect message is sent immediately and no tones are played.
Web: Play Ringback Tone to Trunk [PlayRBTone2Trunk_ID]	<p>Determines the playing of a ringback tone (RBT) to the trunk side and per trunk (where <i>ID</i> depicts the trunk number and 0 is the first trunk). This parameter also determines the method for playing the RBT.</p> <ul style="list-style-type: none"> ▪ [-1] = Not configured - use the value of the parameter PlayRBTone2Tel (default). ▪ [0] Don't Play = The device configured with ISDN/CAS protocol type does not play an RBT. No PI is sent to the ISDN unless the parameter ProgressIndicator2ISDN_ID is configured differently. ▪ [1] Play on Local = The device configured with CAS protocol type plays a local RBT to PSTN upon receipt of a SIP 180 Ringing response (with or without SDP). <p>Note: Receipt of a 183 response does not cause the device configured with CAS to play an RBT (unless SIP183Behaviour is set to 1).</p> <p>The device configured with ISDN protocol type operates according to the parameter LocalISDNRBSorce:</p> <ul style="list-style-type: none"> ✓ If the device receives a 180 Ringing response (with or without SDP) and the parameter LocalISDNRBSorce is set to 1, it plays an RBT and sends an ISDN Alert with PI = 8 (unless the parameter ProgressIndicator2ISDN_ID is configured differently). ✓ If the parameter LocalISDNRBSorce is set to 0, the device doesn't play an RBT and an Alert message (without PI) is sent to the ISDN. In this case, the PBX/PSTN plays the RBT to the originating terminal by itself. <p>Note: Receipt of a 183 response does not cause the device with ISDN protocol type to play an RBT; the device issues a Progress message (unless SIP183Behaviour is set to 1). If the parameter SIP183Behaviour is set to 1, the 183 response is handled the same way as a 180 Ringing response.</p> ▪ [2] Prefer IP = Play according to 'Early Media'. If a SIP 180 response is received and the voice channel is already open (due to a previous 183 early media response or due to an SDP in the current 180 response), the device with ISDN/CAS protocol type doesn't play the RBT; PI = 8 is sent in an ISDN Alert message (unless the parameter ProgressIndicator2ISDN_ID is configured differently). If a 180 response is received, but the 'early media' voice channel is not opened, the device with CAS protocol type plays an RBT to the PSTN. The device with ISDN protocol type operates according to the parameter LocalISDNRBSorce: <ul style="list-style-type: none"> ✓ If LocalISDNRBSorce is set to 1, the device plays an RBT and sends an ISDN Alert with PI = 8 to the ISDN (unless the parameter ProgressIndicator2ISDN_ID is configured differently). ✓ If LocalISDNRBSorce is set to 0, the device doesn't play an RBT. No PI is sent in the ISDN Alert message (unless the parameter ProgressIndicator2ISDN_ID is configured differently). In this case, the PBX/PSTN

Parameter	Description
	<p>should play an RBT tone to the originating terminal by itself.</p> <p>Note: Receipt of a 183 response results in an ISDN Progress message (unless SIP183Behaviour is set to 1). If SIP183Behaviour is set to 1 (183 is handled the same way as a 180 + SDP), the device sends an Alert message with PI = 8, without playing an RBT.</p> <ul style="list-style-type: none"> ▪ [3] Play tone 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. <p>Note: For ISDN trunks, this option is applicable only if LocalISDNRBSources is set to 1.</p>
<p>Web: Digital Out-Of-Service Behavior EMS: Digital OOS Behavior For Trunk Value [DigitalOOSBehaviorForTrunk_ID]</p>	<p>Determines the method for setting digital trunks to Out-Of-Service state per trunk.</p> <ul style="list-style-type: none"> ▪ [-1] Not Configured = Use the settings of the DigitalOOSBehavior parameter for per device (default). ▪ [0] Default = Uses default behavior for each trunk (see note below). ▪ [1] Service = Sends ISDN In or Out of Service (only for ISDN protocols that support Service message). ▪ [2] D-Channel = Takes D-Channel down or up (ISDN only). ▪ [3] Alarm = Sends or clears PSTN AIS Alarm (ISDN and CAS). ▪ [4] Block = Blocks trunk (CAS only). <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only if the parameter EnableBusyOut is set to 1. ▪ The default behavior (value 0) is as follows: <ul style="list-style-type: none"> ✓ ISDN: Use Service messages on supporting variants and use Alarm on non-supporting variants. ✓ CAS: Use Alarm. ▪ When updating this parameter value at run-time, you must stop the trunk and then restart it for the update to take effect. ▪ To determine the method for setting Out-Of-Service state for all trunks (i.e., per device), use the DigitalOOSBehavior parameter. ▪ The <i>ID</i> in the <i>ini</i> file parameter name represents the trunk number, where 0 is the first trunk.
<p>Web: Digital Out-Of-Service Behavior [DigitalOOSBehavior]</p>	<p>Determines the method for setting digital trunks to Out-Of-Service state per device. For a description, see the DigitalOOSBehaviorForTrunk_ID parameter.</p> <p>Note: To configure the method for setting Out-Of-Service state per trunk, use the DigitalOOSBehaviorForTrunk_ID parameter.</p>

Parameter	Description
Web: Default Cause Mapping From ISDN to SIP [DefaultCauseMapISDN2IP]	Defines a single default ISDN release cause that is used (in ISDN-to-IP calls) instead of all received release causes, except when the following Q.931 cause values are received: Normal Call Clearing (16), User Busy (17), No User Responding (18), or No Answer from User (19). The range is any valid Q.931 release cause (0 to 127). The default value is 0 (i.e., not configured - static mapping is used).
Release Cause Mapping from ISDN to SIP Table	
Web: Release Cause Mapping Table EMS: ISDN to SIP Cause Mapping [CauseMapISDN2SIP]	This <i>parameter</i> table maps ISDN Q.850 Release Causes to SIP responses. The format of this parameter is as follows: [CauseMapISDN2SIP] FORMAT CauseMapISDN2SIP_Index = CauseMapISDN2SIP_IsdnReleaseCause, CauseMapISDN2SIP_SipResponse; [\CauseMapISDN2SIP] Where, <ul style="list-style-type: none"> ▪ IsdnReleaseCause = Q.850 Release Cause ▪ SipResponse = SIP Response For example: CauseMapISDN2SIP 0 = 50,480; CauseMapISDN2SIP 0 = 6,406; When a Release Cause is received (from the PSTN side), the device searches this mapping table for a match. If the Q.850 Release Cause is found, the SIP response assigned to it is sent to the IP side. If no match is found, the default static mapping is used. Notes: <ul style="list-style-type: none"> ▪ This parameter can appear up to 12 times. ▪ For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Release Cause Mapping from SIP to ISDN Table	
Web: Release Cause Mapping Table EMS: SIP to ISDN Cause Mapping [CauseMapSIP2ISDN]	This <i>parameter</i> table maps SIP responses to Q.850 Release Causes. The format of this parameter is as follows: [CauseMapSIP2ISDN] FORMAT CauseMapSIP2ISDN_Index = CauseMapSIP2ISDN_SipResponse, CauseMapSIP2ISDN_IsdnReleaseCause; [\CauseMapSIP2ISDN] Where, <ul style="list-style-type: none"> ▪ SipResponse = SIP Response ▪ IsdnReleaseCause = Q.850 Release Cause For example: CauseMapSIP2ISDN 0 = 480,50; CauseMapSIP2ISDN 0 = 404,3; When a SIP response is received (from the IP side), the device searches this mapping table for a match. If the SIP response is found, the Q.850 Release Cause assigned to it is sent to the PSTN. If no match is found, the default static mapping is used. Notes: <ul style="list-style-type: none"> ▪ This parameter can appear up to 12 times.

Parameter	Description
	<ul style="list-style-type: none"> For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Web/EMS: Enable Calling Party Category [EnableCallingPartyCategory]	Determines whether Calling Party Category (CPC) is mapped between SIP and PRI. <ul style="list-style-type: none"> [0] Disable = Don't relay the CPC between SIP and PRI (default). [1] Enable = The CPC is relayed between SIP and PRI. If enabled, the CPC received in the Originating Line Information (OLI) IE of an incoming ISDN Setup message is relayed to the From/P-Asserted-Identity headers using the 'cpc' parameter in the outgoing INVITE message, and vice versa. For example (calling party is a payphone): From:<sip:2000;cpc=payphone@10.8.23.70>;tag=1c1806157451 Note: This feature is applicable only to the NI-2 PRI variant.
[UserToUserHeaderFormat]	Determines the format of the User-to-User SIP header in the INVITE message for interworking the ISDN User to User (UU) IE data to SIP. <ul style="list-style-type: none"> [0] = Format: X-UserToUser (default). [1] = Format: User-to-User with Protocol Discriminator (pd) attribute. User-to-User=3030373435313734313635353b313233343b3834;pd=4. (This format is according to IETF Internet-Draft draft-johnston-sipping-cc-uu-04.) [2] = Format: User-to-User with encoding=hex at the end and pd embedded as the first byte. User-to-User=043030373435313734313635353b313233343b3834;encoding=hex. Where "04" at the beginning of this message is the pd. (This format is according to IETF Internet-Draft draft-johnston-sipping-cc-uu-03.)
Web/EMS: Remove CLI when Restricted [RemoveCLIWhenRestricted]	Determines (for IP-to-Tel calls) whether the Calling Number and Calling Name IEs are removed from the ISDN Setup message if the presentation is set to Restricted. <ul style="list-style-type: none"> [0] No = IE's are not removed (default). [1] Yes = IE's are removed.
Web/EMS: Remove Calling Name [RemoveCallingName]	Enables the device to remove the Calling Name from SIP-to-ISDN calls for all trunks. <ul style="list-style-type: none"> [0] Disable = Does not remove Calling Name (default). [1] Enable = Removes Calling Name.
Web: Remove Calling Name EMS: Remove Calling Name For Trunk Mode [RemoveCallingNameForTrunk_x]	Enables the device to remove the Calling Name per trunk (where x denotes the trunk number) for SIP-to-ISDN calls. <ul style="list-style-type: none"> [-1] Use Global Parameter = Settings of the global parameter RemoveCallingName are used (default). [0] Disable = Does not remove Calling Name. [1] Enable = Remove Calling Name.
Web/EMS: Progress Indicator to ISDN [ProgressIndicator2ISDN_ID]	Determines the Progress Indicator (PI) to ISDN. The <i>ID</i> in the <i>ini</i> file parameter depicts the trunk number, where 0 is the first trunk.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [-1] Not Configured = The PI in ISDN messages is set according to the parameter PlayRBTone2Tel (default). ▪ [0] No PI = PI is not sent to ISDN. ▪ [1] PI = 1; [8] PI = 8: The PI value is sent to PSTN in Q.931/Proceeding and Alerting messages. Typically, the PSTN/PBX cuts through the audio channel without playing local Ringback tone, enabling the originating party to hear remote Call Progress Tones or network announcements.
Web: Set PI in Rx Disconnect Message EMS: Set PI For Disconnect Msg [PIForDisconnectMsg_ID]	Defines the device's behavior when a Disconnect message is received from the ISDN before a Connect message is received. The <i>ID</i> in the <i>ini</i> file parameter depicts the trunk number, where 0 is the first trunk. <ul style="list-style-type: none"> ▪ [-1] Not Configured = Sends a 183 SIP response according to the received progress indicator (PI) in the ISDN Disconnect message. If PI = 1 or 8, the device sends a 183 response, enabling the PSTN to play a voice announcement to the IP side. If there isn't a PI in the Disconnect message, the call is released (default). ▪ [0] No PI = Doesn't send a 183 response to IP. The call is released. ▪ [1] PI = 1; [8] PI = 8: Sends a 183 response to IP.
EMS: Connect On Progress Ind [ConnectOnProgressInd]	Enables the play of announcements from IP to PSTN without the need to answer the Tel-to-IP call. It can be used with PSTN networks that don't support the opening of a TDM channel before an ISDN Connect message is received. <ul style="list-style-type: none"> ▪ [0] = Connect message isn't sent after SIP 183 Session Progress message is received (default). ▪ [1] = Connect message is sent after SIP 183 Session Progress message is received.
Web: Local ISDN Ringback Tone Source EMS: Local ISDN RB Source [LocalISDNRBSource_ID]	Determines whether the Ringback tone is played to the ISDN by the PBX/PSTN or by the device. <ul style="list-style-type: none"> ▪ [0] PBX = PBX/PSTN (default). ▪ [1] Gateway = device plays the Ringback tone. This parameter is applicable to ISDN protocols. It is used simultaneously with the parameter PlayRBTone2Trunk. The <i>ID</i> in the <i>ini</i> file parameter depicts the trunk number, where 0 is the first trunk.
Web/EMS: PSTN Alert Timeout [TrunkPSTNAlertTimeout_ID]	Defines the Alert Timeout (ISDN T301 timer) in seconds for outgoing calls to PSTN. This timer is used between the time that an ISDN Setup message is sent to the Tel side (IP-to-Tel call establishment) and a Connect message is received. If Alerting is received, the timer is restarted. In the <i>ini</i> file parameter, <i>ID</i> depicts the trunk number, where 0 is the first trunk. The range is 1 to 600. The default is 180.
Web: B-Channel Negotiation EMS: B-Channel Negotiation For Trunk Mode [BChannelNegotiationForTrunk_x]	Determines the ISDN B-channel negotiation mode. <ul style="list-style-type: none"> ▪ [-1] Not Configured = use per device configuration of the BChannelNegotiation parameter (default). ▪ [0] Preferred = Preferred. ▪ [1] Exclusive = Exclusive. ▪ [2] Any = Any.

Parameter	Description
	<p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable to ISDN protocols. ▪ The option 'Any' is only applicable if TerminationSide is set to 0 (i.e., User side). ▪ The x represents the trunk number, where 0 is the first trunk.
[SendISDNServiceAfterRestart]	<p>Enables the device to send an ISDN SERVICE message per trunk upon device reset. The message (transmitted on the trunk's D-channel) indicates the availability of the trunk's B-channels (i.e., trunk in service).</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default). ▪ [1] = Enable.
EMS: Support Redirect InFacility [SupportRedirectInFacility]	<p>Determines whether the Redirect Number is retrieved from the Facility IE.</p> <ul style="list-style-type: none"> ▪ [0] = Not supported (default). ▪ [1] = Supports partial retrieval of Redirect Number (number only) from the Facility IE in ISDN Setup messages. This is applicable to Redirect Number according to ECMA-173 Call Diversion Supplementary Services. <p>Note: To enable this feature, the parameter ISDNDuplicateQ931BuffMode must be set to 1.</p>
[CallReroutingMode]	<p>Determines whether ISDN call rerouting (call forward) is performed by the PSTN instead of by the SIP side. This call forwarding is based on Call Deflection for Euro ISDN (ETS-300-207-1) and QSIG (ETSI TS 102 393).</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable = Enables ISDN call rerouting. When the device sends the INVITE message to the remote SIP entity and receives a SIP 302 response with a Contact header containing a URI host name that is the same as the device's IP address, the device sends a Facility message with a Call Rerouting invoke method to the ISDN and waits for the PSTN side to disconnect the call. <p>Note: When this parameter is enabled, ensure that you configure in the Inbound IP Routing Table' (PSTNPrefix ini file parameter) a rule to route the redirected call (using the user part from the 302 Contact header) to the same Trunk Group from where the incoming Tel-to-IP call was received.</p>
EMS: Enable CIC [EnableCIC]	<p>Determines whether the Carrier Identification Code (CIC) is relayed to ISDN.</p> <ul style="list-style-type: none"> ▪ [0] = Do not relay the Carrier Identification Code (CIC) to ISDN (default). ▪ [1] = CIC is relayed to the ISDN in Transit Network Selection (TNS) IE. <p>If enabled, the CIC code (received in an INVITE Request-URI) is included in a TNS IE in the ISDN Setup message. For example: INVITE sip:555666;cic=2345@100.2.3.4 sip/2.0.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This feature is supported only for SIP-to-ISDN calls. ▪ The parameter AddCicAsPrefix can be used to add the CIC as a prefix to the destination phone number for routing IP-to-

Parameter	Description
	Tel calls.
EMS: Enable AOC [EnableAOC]	Determines whether ISDN Advice of Charge (AOC) messages are interworked with SIP. <ul style="list-style-type: none"> ▪ [0] = Not used (default). ▪ [1] = AOC messages are interworked to SIP (in receive direction) and sent to the PSTN in the transmit direction. The device supports both the receipt and sending of ISDN (Euro ISDN) AOC messages: <ul style="list-style-type: none"> ▪ AOC messages can be received during a call (Facility messages) or at the end of a call (Disconnect or Release messages). The device converts the AOC messages into SIP INFO (during a call) and BYE (end of a call) messages, using a proprietary AOC SIP header. The device supports both Currency and Pulse AOC messages. ▪ AOC messages can be sent during a call (Facility messages) or at the end of a call (Disconnect or Release messages). This is done by assigning the Charge Code index to the desired routing rule in the Outbound IP Routing table. For more information, see 'Advice of Charge Services for Euro ISDN' on page 310.
Web: IPMedia Detectors EMS: DSP Detectors Enable [EnableDSPIPMDetectors]	Enables the device's DSP detectors. <ul style="list-style-type: none"> ▪ [0] = Disable (default). ▪ [1] = Enable. Notes: <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ The device's Software Upgrade Key must contain the 'IPMDetector' DSP option. ▪ When enabled (1), the number of available channels is reduced.
Web: Add IE in SETUP EMS: IE To Be Added In Q.931 Setup [AddIEinSetup]	Adds an optional Information Element (IE) data (in hex format) to ISDN Setup messages. For example, to add IE '0x20,0x02,0x00,0xe1', enter the value "200200e1". Notes: <ul style="list-style-type: none"> ▪ This IE is sent from the Trunk Group IDs that are defined by the parameter SendIEonTG. ▪ You can configure different IE data for Trunk Groups by defining this parameter for different IP Profile IDs (using the IPProfile parameter) and then assigning the required IP Profile ID in the Inbound IP Routing Table' (PSTNPrefix).
Web: Trunk Groups to Send IE EMS: List Of Trunk Groups To Send IE [SendIEonTG]	Defines Trunk Group IDs (up to 50 characters) from where the optional ISDN IE (defined by the parameter AddIEinSetup) is sent. For example: '1,2,4,10,12,6'. Notes: <ul style="list-style-type: none"> ▪ You can configure different IE data for Trunk Groups by defining this parameter for different IP Profile IDs (using the parameter IPProfile), and then assigning the required IP Profile ID in the Inbound IP Routing Table' (PSTNPrefix). ▪ When IP Profiles are used for configuring different IE data for Trunk Groups, this parameter is ignored.
Web: Enable User-to-User IE for Tel to IP	Enables ISDN PRI-to-SIP interworking. <ul style="list-style-type: none"> ▪ [0] Disable = Disabled (default).

Parameter	Description				
EMS: Enable UUI Tel 2 Ip [EnableUUITel2IP]	<ul style="list-style-type: none"> [1] Enable = Enable transfer of User-to-User (UU) IE from PRI to SIP. <p>The device supports the following ISDN PRI-to-SIP interworking: Setup to SIP INVITE, Connect to SIP 200 OK, User Information to SIP INFO, Alerting to SIP 18x response, and Disconnect to SIP BYE response messages.</p> <p>Note: The interworking of ISDN User-to-User IE to SIP INFO is applicable only to the Euro ISDN, QSIG, and 4ESS PRI variants.</p>				
Web: Enable User-to-User IE for IP to Tel EMS: Enable UUI Ip 2 Tel [EnableUUIIP2Tel]	<p>Enables SIP-to-PRI ISDN interworking.</p> <ul style="list-style-type: none"> [0] Disable = Disabled (default). [1] Enable = Enable transfer of User-to-User (UU) IE from SIP INVITE message to PRI Setup message. <p>The device supports the following SIP-to-PRI ISDN interworking: SIP INVITE to Setup, SIP 200 OK to Connect, SIP INFO to User Information, SIP 18x to Alerting, and SIP BYE to Disconnect.</p> <p>Notes:</p> <ul style="list-style-type: none"> The interworking of ISDN User-to-User IE to SIP INFO is applicable only to the Euro ISDN, QSIG, and 4ESS PRI variants. To interwork the UUIE header from SIP-to-ISDN messages with the 4ESS ISDN variant, the parameter ISDNGeneralCCBehavior must be set to 16384. 				
[Enable911LocationIdIP2Tel]	<p>Enables interworking of Emergency Location Identification from SIP to PRI.</p> <ul style="list-style-type: none"> [0] = Disabled (default) [1] = Enabled <p>When enabled, the From header received in the SIP INVITE is translated into the following ISDN IE's:</p> <ul style="list-style-type: none"> Emergency Call Control. Generic Information - to carry the Location Identification Number information. Generic Information - to carry the Calling Geodetic Location information. <p>Note: This capability is applicable only to the NI-2 ISDN variant.</p>				
[EarlyAnswerTimeout]	<p>Defines the time (in seconds) that the device waits for an ISDN Connect message from the called party (Tel side) after sending a Setup message. If the timer expires, the call is answered by sending a SIP 200 OK message (IP side).</p> <p>The valid range is 0 to 600. The default value is 0 (i.e., disabled).</p>				
Web/EMS: Trunk Transfer Mode [TrunkTransferMode]	<p>Determines the trunk transfer method (for all trunks) when a SIP REFER message is received. The transfer method depends on the Trunk's PSTN protocol (configured by the parameter ProtocolType) and is applicable only when one of these protocols are used:</p> <table border="1" data-bbox="641 1935 1401 1980"> <thead> <tr> <th data-bbox="641 1935 932 1980">PSTN Protocol</th> <th data-bbox="932 1935 1401 1980">Transfer Method (Described Below)</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	PSTN Protocol	Transfer Method (Described Below)		
PSTN Protocol	Transfer Method (Described Below)				

Parameter	Description	
	E1 Euro ISDN [1]	ECT [2] or InBand [5]
	E1 QSIG [21], T1 QSIG [23]	Single Step Transfer [4], Path Replacement Transfer [2], or InBand [5]
	T1 NI2 ISDN [10], T1 4ESS ISDN [11], T1 5ESS 9 ISDN [12]	TBCT [2] or InBand [5]
	T1 DMS-100 ISDN [14]	RTL [2] or InBand [5]
	T1 RAW CAS [3], T1 CAS [2], E1 CAS [8], E1 RAW CAS [9]	[1] CAS NFA DMS-100 or [3] CAS Normal transfer
	T1 DMS-100 Meridian ISDN [35]	RTL [2] or InBand [5]
<p>The valid values of this parameter are described below:</p> <ul style="list-style-type: none"> ▪ [0] = Not supported (default). ▪ [1] = Supports CAS NFA DMS-100 transfer. When a SIP REFER message is received, the device performs a Blind Transfer by executing a CAS Wink, waits for an acknowledged Wink from the remote side, dials the Refer-to number to the switch, and then releases the call. Note: A specific NFA CAS table is required. ▪ [2] = Supports ISDN (PRI/BRI) transfer - Release Link Trunk (RLT) (DMS-100), Two B Channel Transfer (TBCT) (NI2), Explicit Call Transfer (ECT) (EURO ISDN), and Path Replacement (QSIG). When a SIP REFER message is received, the device performs a transfer by sending Facility messages to the PBX with the necessary information on the call's legs to be connected. The different ISDN variants use slightly different methods (using Facility messages) to perform the transfer. Notes: <ul style="list-style-type: none"> ✓ For RLT ISDN transfer, the parameter <code>SendISDNTransferOnConnect</code> must be set to 1. ✓ The parameter <code>SendISDNTransferOnConnect</code> can be used to define if the TBCT/ECT transfer is performed after receipt of Alerting or Connect messages. For RLT, the transfer is always done after receipt of Connect (<code>SendISDNTransferOnConnect</code> is set to 1). ✓ This transfer can be performed between B-channels from different trunks or Trunk Groups, by using the parameter <code>EnableTransferAcrossTrunkGroups</code>. ✓ The device initiates the ECT process after receiving a SIP REFER message only for trunks that are configured to User side. ▪ [3] = Supports CAS Normal transfer. When a SIP REFER message is received, the device performs a Blind Transfer by executing a CAS Wink, dialing the Refer-to number to the switch, and then releasing the call. ▪ [4] = Supports QSIG Single Step transfer (PRI/BRI): IP-to-Tel: When a SIP REFER message is received, the 		

Parameter	Description
	<p>device performs a transfer by sending a Facility message to the PBX, initiating Single Step transfer. Once a success return result is received, the transfer is completed.</p> <p>Tel-to-IP: When a Facility message initiating Single Step transfer is received from the PBX, a SIP REFER message is sent to the IP side.</p> <ul style="list-style-type: none"> ▪ [5] = IP-to-Tel Blind Transfer mode supported for ISDN (PRI/BRI) protocols and implemented according to AT&T Toll Free Transfer Connect Service (TR 50075) "Courtesy Transfer-Human-No Data". When the device receives a SIP REFER message, it performs a blind transfer by first dialing the DTMF digits (transfer prefix) defined by the parameter XferPrefixIP2Tel (configured to "*8" for AT&T service), and then (after 500 msec) the device dials the DTMF of the number (referred) from the Refer-To header sip:URI userpart. <p>If the hostpart of the Refer-To sip:URI contains the device's IP address, and if the Trunk Group selected according to the IP to Tel Routing table is the same Trunk Group as the original call, then the device performs the in-band DTMF transfer; otherwise, the device sends the INVITE according to regular transfer rules.</p> <p>After completing the in-band transfer, the device waits for the ISDN Disconnect message. If the Disconnect message is received during the first 5 seconds, the device sends a SIP NOTIFY with 200 OK message; otherwise, the device sends a NOTIFY with 4xx message.</p> <ul style="list-style-type: none"> ▪ [6] = Supports AT&T toll free out-of-band blind transfer for trunks configured with the 4ESS ISDN protocol. AT&T courtesy transfer is a supplementary service which enables a user (e.g., user "A") to transform an established call between it and user "B" into a new call between users "B" and "C", whereby user "A" does not have a call established with user "C" prior to call transfer. The device handles this feature as follows: <ul style="list-style-type: none"> ✓ IP-to-Tel (user side): When a SIP REFER message is received, the device initiates a transfer by sending a Facility message to the PBX. ✓ Tel-to-IP (network side): When a Facility message initiating an out-of-band blind transfer is received from the PBX, the device sends a SIP REFER message to the IP side (if the EnableNetworkISDNTransfer parameter is set to 1). <p>Note: For configuring trunk transfer mode per trunk, use the parameter TrunkTransferMode_X.</p>
[TrunkTransferMode_X]	Determines the trunk transfer mode per trunk (where x is the Trunk ID). For configuring trunk transfer mode for all trunks and for a description of the parameter options, refer to the parameter TrunkTransferMode.
[EnableTransferAcrossTrunkGroups]	<p>Determines whether the device allows ISDN ECT, RLT or TBCT IP-to-Tel call transfers between B-channels of different Trunk Groups.</p> <ul style="list-style-type: none"> ▪ [0] = Disable - ISDN call transfer is only between B-channels of the same Trunk Group (default).

Parameter	Description
	<ul style="list-style-type: none"> ▪ [1] = Enable - the device performs ISDN transfer between any two PSTN calls (between any Trunk Group) handled by the device. <p>Note: The ISDN transfer also requires that you configure the parameter <code>TrunkTransferMode_x</code> to 2.</p>
Web: ISDN Transfer Capabilities EMS: Transfer Capability To ISDN [ISDNTransferCapability_ID]	Defines the IP-to-ISDN Transfer Capability of the Bearer Capability IE in ISDN Setup messages. The <i>ID</i> in the ini file parameter depicts the trunk number, where 0 is the first trunk. <ul style="list-style-type: none"> ▪ [-1] Not Configured ▪ [0] Audio 3.1 = Audio (default). ▪ [1] Speech = Speech. ▪ [2] Data = Data. ▪ Audio 7 = Currently not supported. <p>Note: If this parameter isn't configured or equals to '-1', Audio 3.1 capability is used.</p>
Web: ISDN Transfer On Connect EMS: Send ISDN Transfer On Connect [SendISDNTransferOnConnect]	This parameter is used for the ECT/TBCT/RLT/Path Replacement ISDN transfer methods. Usually, the device requests the PBX to connect an incoming and outgoing call. This parameter determines if the outgoing call (from the device to the PBX) must be connected before the transfer is initiated. <ul style="list-style-type: none"> ▪ [0] Alert = Enables ISDN Transfer if the outgoing call is in Alerting or Connect state (default). ▪ [1] Connect = Enables ISDN Transfer only if the outgoing call is in Connect state. <p>Note: For RLT ISDN transfer (<code>TrunkTransferMode = 2</code> and <code>ProtocolType = 14 DMS-100</code>), this parameter must be set to 1.</p>
[ISDNTransferCompleteTimeout]	Defines the timeout (in seconds) for determining ISDN call transfer (ECT, RLT, or TBCT) failure. If the device does not receive any response to an ISDN transfer attempt within this user-defined time, the device identifies this as an ISDN transfer failure and subsequently performs a hairpin TDM connection or sends a SIP NOTIFY message with a SIP 603 response (depending whether hairpin is enabled or disabled, using the parameter <code>DisableFallbackTransferToTDM</code>). The valid range is 1 to 10. The default is 4.
Web/EMS: Enable Network ISDN Transfer [EnableNetworkISDNTransfer]	Determines whether the device allows interworking of network-side received ECT/TBCT Facility messages (NI2 TBCT - Two B-channel Transfer and ETSI ECT - Explicit Call Transfer) to SIP REFER. <ul style="list-style-type: none"> ▪ [0] Disable = Rejects ISDN transfer requests. ▪ [1] Enable (default) = The device sends a SIP REFER message to the remote call party if ECT/TBCT Facility messages are received from the ISDN side (e.g., from a PBX).
[DisableFallbackTransferToTDM]	Enables "hairpin" TDM transfer upon ISDN (ECT, RLT, or TBCT) call transfer failure. When this feature is enabled and an ISDN call transfer failure occurs, the device sends a SIP NOTIFY message with a SIP 603 Decline response. <ul style="list-style-type: none"> ▪ [0] = device performs a hairpin TDM transfer upon ISDN call transfer (default). ▪ [1] = Hairpin TDM transfer is disabled.

Parameter	Description
Web: Enable QSIG Transfer Update [EnableQSIGTransferUpdate]	<p>Determines whether the device interworks QSIG Facility messages with callTransferComplete invoke application protocol data unit (APDU) to SIP UPDATE messages with P-Asserted-Identity and optional Privacy headers. This feature is supported for IP-to-Tel and Tel-to-IP calls.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) = Ignores QSIG Facility message with callTransferComplete invoke ▪ [1] Enable <p>For example, assume A and C are PBX call parties, and B is the SIP IP phone:</p> <ol style="list-style-type: none"> 1 A calls B; B answers the call. 2 A places B on hold, and calls C; C answers the call. 3 A performs a call transfer (the transfer is done internally by the PBX); B and C are connected to one another. <p>In the above example, the PBX updates B that it is now talking with C. The PBX updates this by sending a QSIG Facility message with callTransferComplete invoke APDU. The device interworks this message to a SIP UPDATE message containing a P-Asserted-Identity header with the number and name derived from QSIG callTransferComplete redirectionNumber and redirectionName.</p> <p>Note: For IP-to-Tel calls, the redirectionNumber and redirectionName in the callTransferComplete invoke is derived from the P-Asserted-Identity and Privacy headers.</p>
[CASSendHookFlash]	<p>Enables sending Wink signal toward CAS trunks.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default). ▪ [1] = Enable. <p>If the device receives a mid-call SIP INFO message with flashhook event body (as shown below) and this parameter is set to 1, the device generates a wink signal toward the CAS trunk. The CAS wink signal is done by changing the A bit from 1 to 0, and then back to 1 for 450 msec.</p> <pre style="background-color: #f0f0f0; padding: 5px;">INFO sip:4505656002@192.168.13.40:5060 SIP/2.0 Via: SIP/2.0/UDP 192.168.13.2:5060 From: <sip:06@192.168.13.2:5060> To: <sip:4505656002@192.168.13.40:5060>;tag=13287 8796-1040067870294 Call-ID: 0010-0016-D69A7DA8-1@192.168.13.2 CSeq:2 INFO Content-Type: application/broadsoft Content-Length: 17 event flashhook</pre> <p>Note: This parameter is applicable only to T1 CAS protocols.</p>

A.12.8 Answer and Disconnect Supervision Parameters

The answer and disconnect supervision parameters are described in the table below.

Table A-60: 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. <ul style="list-style-type: none"> ▪ [1] Yes = The device sends a SIP 200 OK (in response to an INVITE message) when speech, fax, or modem is detected from the Tel side. ▪ [0] No = The device sends a SIP 200 OK only after it completes dialing to the Tel side (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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ FXO interfaces: This feature is applicable only to one-stage dialing (FXO). ▪ Digital interfaces: To activate this feature, set the EnableDSPIPMDetectors parameter to 1. ▪ Digital interfaces: This feature is applicable only when the protocol type is CAS.
Web/EMS: Max Call Duration (min) [MaxCallDuration]	Defines the maximum duration (in minutes) of a call. If this duration is reached, the device terminates the call. This feature is useful for ensuring available resources for new calls, by ensuring calls are properly terminated. 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. <ul style="list-style-type: none"> ▪ [0] Disable = Call is not released (default). ▪ [1] Enable = Call is released if dial tone is detected on the device's FXO port. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.
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/CAS.
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. <ul style="list-style-type: none"> ▪ [0] No ▪ [1] Yes (default) <p>Notes:</p> <ul style="list-style-type: none"> ▪ The timeout is configured by the BrokenConnectionEventTimeout parameter.

Parameter	Description
	<ul style="list-style-type: none"> ▪ 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 217).
Web: Broken Connection Timeout EMS: Broken Connection Event Timeout [BrokenConnectionEventTimeout]	Defines 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: <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> ▪ [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.
Web: Silence Detection Period [sec] EMS: Silence Detection Time Out [FarEndDisconnectSilencePeriod]	Defines the duration of the silence period (in seconds) after which the call is disconnected. The range is 10 to 28,800 (i.e., 8 hours). The default is 120 seconds. Note: For this parameter to take effect, a device reset is required.
Web: Silence Detection Method [FarEndDisconnectSilenceMethod]	Determines the silence detection method. <ul style="list-style-type: none"> ▪ [0] None = Silence detection option is disabled. ▪ [1] Packets Count = According to packet count. ▪ [2] Voice/Energy Detectors = N/A. ▪ [3] All = N/A. Note: For this parameter to take effect, a device reset is required.
[FarEndDisconnectSilenceThreshold]	Defines the threshold of the packet count (in percentages) below which is considered silence by the device. The valid range is 1 to 100%. The default is 8%. Notes: <ul style="list-style-type: none"> ▪ This parameter is applicable only if silence is detected

Parameter	Description
	according to packet count (FarEndDisconnectSilenceMethod is set to 1). <ul style="list-style-type: none"> ▪ 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. <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable.
Web: Trunk Alarm Call Disconnect Timeout [TrunkAlarmCallDisconnectTimeout]	Defines the time (in seconds) to wait (in seconds) after an E1/T1 trunk "red" alarm (LOS/LOF) is raised before the device disconnects the SIP call. Once this user-defined time elapses, the device sends a SIP BYE message to terminate the call. If the alarm is cleared before this timeout elapses, the call is not terminated and continues as normal. The range is 1 to 80. The default is 0 (20 for E1 and 40 for T1).
Web: Disconnect Call on Busy Tone Detection (ISDN) EMS: Isdn Disconnect On Busy Tone [ISDNDisconnectOnBusyTone]	Determines whether a call is disconnected upon detection of a busy tone (for ISDN). <ul style="list-style-type: none"> ▪ [0] Disable = Do not disconnect call upon detection of busy tone. ▪ [1] Enable = Disconnect call upon detection of busy tone (default). Notes: <ul style="list-style-type: none"> ▪ This parameter is applicable only to ISDN protocols. ▪ IP-to-ISDN calls are disconnected on detection of SIT tones only in call alert state. If the call is in connected state, the SIT does not disconnect the calls. Detection of Busy or Reorder tones disconnects the IP-to-ISDN calls also in call connected state. ▪ For IP-to-CAS calls, detection of Busy, Reorder or SIT tones disconnect the calls in any call state.
Web: Disconnect Call on Busy Tone Detection (CAS) EMS: Disconnect On Detection End Tones [DisconnectOnBusyTone]	Determines whether a call is disconnected upon detection of a busy tone (for CAS). <ul style="list-style-type: none"> ▪ [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: <ul style="list-style-type: none"> ▪ Digital interfaces: This parameter is applicable only to CAS protocols. ▪ Analog interfaces: This parameter is applicable only to FXO interfaces. ▪ This parameter can also be configured per Tel Profile, using the TelProfile parameter.
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. <ul style="list-style-type: none"> ▪ [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.

Parameter	Description
	<p>The FXO interface sends a 200 OK response when polarity reversal signal is detected (applicable only to one-stage dialing) and releases a call when a second polarity reversal signal is detected.</p> <p>Note: This parameter can also be configured per Tel Profile, using the TelProfile parameter.</p>
<p>Web/EMS: Enable Current Disconnect [EnableCurrentDisconnect]</p>	<p>Enables call release upon detection of a Current Disconnect signal.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable the current disconnect service (default). ▪ [1] Enable = Enable the current disconnect service. <p>If the current disconnect service is enabled:</p> <ul style="list-style-type: none"> ▪ 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. <p>The current disconnect duration is configured by the CurrentDisconnectDuration parameter. The current disconnect threshold (FXO only) is configured by the CurrentDisconnectDefaultThreshold parameter. The frequency at which the analog line voltage is sampled is configured by the TimeToSampleAnalogLineVoltage parameter.</p> <p>Note: This parameter can also be configured per Tel Profile, using the TelProfile parameter.</p>
<p>EMS: Polarity Reversal Type [PolarityReversalType]</p>	<p>Defines the voltage change slope during polarity reversal or wink.</p> <ul style="list-style-type: none"> ▪ [0] = Soft reverse polarity (default). ▪ [1] = Hard reverse polarity. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.
<p>EMS: Current Disconnect Duration [CurrentDisconnectDuration]</p>	<p>Defines the duration (in msec) of the current disconnect pulse. The range is 200 to 1500. The default is 900.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.
<p>[CurrentDisconnectDefaultThreshold]</p>	<p>Defines 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.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only to FXO interfaces. ▪ For this parameter to take effect, a device reset is required.
<p>[TimeToSampleAnalogLineVoltage]</p>	<p>Defines the frequency at which the analog line voltage is sampled (after offhook), for detection of the current disconnect threshold.</p>

Parameter	Description
	The valid range is 100 to 2500 msec. The default value is 1000 msec. Notes: <ul style="list-style-type: none"> This parameter is applicable only to FXO interfaces. For this parameter to take effect, a device reset is required.

A.12.9 Tone Parameters

This subsection describes the device's tone parameters.

A.12.9.1 Telephony Tone Parameters

The telephony tone parameters are described in the table below.

Table A-61: Tone Parameters

Parameter	Description
[EnableMOH]	Enables the option for using an external audio source that is connected to the device's AUDIO connector (on the CPU module). When enabled, the device uses the incoming audio from this connector instead of playing the Held Tone defined in the Call Progress Tones (CPT) file. <ul style="list-style-type: none"> [0] = Disable (default). [1] = Enable. Note: EnableHold must be set to 1 to enable this feature.
[PlayHeldToneForIP2IP]	Enables playing a Held tone to an IP-to-IP leg instead of putting it on hold. <ul style="list-style-type: none"> [0] = Disabled. The device interworks the re-INVITE with a=inactive from one SIP leg to another SIP leg. (default) [1] = Enabled. The device plays a Held tone to the IP if it receives a re-INVITE with a=inactive in the SDP from the party initiating the call hold. The Held tone must be configured in the CPT or PRT file. Note: This parameter is applicable only to the IP-to-IP application (enabled using the parameter EnableIP2IPApplication).
Web/EMS: Dial Tone Duration [sec] [TimeForDialTone]	Defines the duration (in seconds) that the dial tone is played (for digital interfaces, to an ISDN terminal). For digital interfaces: This parameter is applicable for overlap dialing when ISDNInCallsBehavior is set to 65536. The dial tone is played if the ISDN Setup message doesn't include the called number. The valid range is 0 to 60. The default is 5. For analog interfaces: FXS interfaces play the dial tone after the phone is picked up (off-hook). FXO interfaces play the dial tone after the port is seized in response to ringing (from PBX/PSTN). The valid range is 0 to 60. The default time is 16. Notes for analog interfaces: <ul style="list-style-type: none"> 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]	Defines the duration (in msec) of the Confirmation tone. A Stutter tone is played (instead of a regular dial tone) when a Message Waiting Indication (MWI) is received. The Stutter tone is composed of a Confirmation tone (Tone Type #8), which is played for the defined

Parameter	Description
	<p>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).</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 more information on MWI, see Message Waiting Indication on page 293.
<p>Web: FXO AutoDial Play BusyTone EMS: Auto Dial Play Busy Tone [FXOAutoDialPlayBusyTone]</p>	<p>Determines whether the device plays a Busy/Reorder tone to the PSTN side if a Tel-to-IP call is rejected by a SIP error response (4xx, 5xx or 6xx). If a SIP error response is received, the device seizes the line (off-hook), and then plays a Busy/Reorder tone to the PSTN side (for the duration defined by the parameter TimeForReorderTone). After playing the tone, the line is released (on-hook).</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable <p>Note: This parameter is applicable only to FXO interfaces.</p>
<p>Web: Hotline Dial Tone Duration EMS: Hot Line Tone Duration [HotLineToneDuration]</p>	<p>Defines the duration (in seconds) of the Hotline dial tone. If no digits are received during this duration, the device initiates a call to a user-defined number (configured in the Automatic Dialing table - TargetOfChannel - see Configuring Automatic Dialing on page 317). The valid range is 0 to 60. The default is 16.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable to FXS and FXO interfaces. ▪ You can define the Hotline duration per FXS/FXO port using the Automatic Dialing table.
<p>Web/EMS: Reorder Tone Duration [sec] [TimeForReorderTone]</p>	<p>For Analog: Defines 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.</p> <p>For Digital: Defines the duration (in seconds) that the CAS device plays a Busy or Reorder Tone before releasing the line. The valid range is 0 to 254. The default value is 10.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The selection of Busy or Reorder tone is performed according to the release cause received from IP. ▪ This parameter is also applicable for ISDN when PlayBusyTone2ISDN is set to 2. ▪ This parameter can also be configured per Tel Profile, using the TelProfile parameter).
<p>Web: Time Before Reorder Tone [sec] EMS: Time For Reorder Tone [TimeBeforeReorderTone]</p>	<p>Defines the delay interval (in seconds) from when the device receives a SIP BYE message (i.e., remote party terminates call) until the device starts playing a Reorder tone to the FXS phone. The valid range is 0 to 60. The default is 0.</p> <p>Note: This parameter is applicable only to FXS interfaces.</p>
<p>Web: Cut Through Reorder</p>	<p>Defines the duration (in seconds) of the Reorder tone played to the</p>

Parameter	Description
Tone Duration [sec] [CutThroughTimeForReOrderTone]	PSTN side after the IP call party releases the call, for the Cut-Through feature. After the tone stops playing, an incoming call is immediately answered if the FXS is off-hooked (for analog interfaces) or the PSTN is connected (for digital interfaces). 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 DigitalCutThrough (for CAS channels) or CutThrough (for FXS channels) parameters.
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. <ul style="list-style-type: none"> ▪ [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. Notes: <ul style="list-style-type: none"> ▪ A negative value indicates that the tone is played infinitely. ▪ This parameter is applicable only to analog interfaces.
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. <ul style="list-style-type: none"> ▪ [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. Note: For ISDN trunks, this option is applicable only if the parameter LocalISDNRBSources is set to 1. Note: This parameter is also applicable to the IP2IP application.
Web: Play Ringback Tone to IP EMS: Play Ring Back Tone To IP [PlayRBTone2IP]	Determines whether the device plays a ringback tone (RBT) to the IP side for IP-to-Tel calls. <ul style="list-style-type: none"> ▪ [0] Don't Play = Ringback tone isn't played (default). ▪ [1] Play = Ringback tone is played after SIP 183 session progress response is sent. For digital modules: If configured to 1 ('Play') and EnableEarlyMedia is set to 1, the device plays a ringback tone according to the following: <ul style="list-style-type: none"> ▪ For CAS interfaces: the device opens a voice channel, sends a 183+SDP response, and then plays a ringback tone to IP. ▪ For ISDN interfaces: if a Progress or an Alerting message with PI (1

Parameter	Description
	<p>or 8) is received from the ISDN, the device opens a voice channel, sends a 183+SDP or 180+SDP response, but doesn't play a ringback tone to IP. If PI (1 or 8) is received from the ISDN, the device assumes that ringback tone is played by the ISDN switch. Otherwise, the device plays a ringback tone to IP after receiving an Alerting message from the ISDN. It sends a 180+SDP response, signaling to the calling party to open a voice channel to hear the played ringback tone.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 217).
<p>Web: Play Local RBT on ISDN Transfer EMS: Play RBT On ISDN Transfer [PlayRBTOnISDNTransfer]</p>	<p>Determines whether the device plays a local ringback tone (RBT) for ISDN's Two B Channel Transfer (TBCT), Release Line Trunk (RLT), or Explicit Call Transfer (ECT) call transfers to the originator when the second leg receives an ISDN Alerting or Progress message.</p> <ul style="list-style-type: none"> ▪ [0] Don't Play (default). ▪ [1] Play. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For Blind transfer, the local RBT is played to first call PSTN party when the second leg receives the ISDN Alerting or Progress message. ▪ For Consulted transfer, the local RBT is played when the second leg receives ISDN Alerting or Progress message if the Progress message is received after a SIP REFER. ▪ This parameter is applicable only if the parameter SendISDNTransferOnConnect is set to 1.
<p>Web: MFC R2 Category EMS: R2 Category [R2Category]</p>	<p>Defines the tone for MFC R2 calling party category (CPC). The parameter provides information on the calling party such as National or International call, Operator or Subscriber and Subscriber priority. The value range is 1 to 15 (defining one of the MFC R2 tones). The default value is 1.</p>
Tone Index Table	
<p>[ToneIndex]</p>	<p>This parameter table 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.</p> <p>The format of this parameter is as follows:</p> <pre>[ToneIndex] FORMAT ToneIndex_Index = ToneIndex_FXSPort_First, ToneIndex_FXSPort_Last, ToneIndex_SourcePrefix, ToneIndex_DestinationPrefix, ToneIndex_PriorityIndex; [ToneIndex]</pre> <p>Where,</p> <ul style="list-style-type: none"> ▪ FXSPort_First = starting range of FXS ports (where 1 is the first

Parameter	Description
	<p>port).</p> <ul style="list-style-type: none"> ▪ 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): <ul style="list-style-type: none"> ✓ 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. <p>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;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.

A.12.9.2 Tone Detection Parameters

The signal tone detection parameters are described in the table below.

Table A-62: Tone Detection Parameters

Parameter	Description
EMS: DTMF Enable [DTMFDetectorEnable]	Enables the detection of DTMF signaling. <ul style="list-style-type: none"> ▪ [0] = Disable ▪ [1] = Enable (default)
EMS: MF R1 Enable [MFR1DetectorEnable]	Enables the detection of MF-R1 signaling. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable
EMS: R1.5 Detection Standard [R1DetectionStandard]	Determines the MF-R1 protocol used for detection. <ul style="list-style-type: none"> ▪ [0] = ITU (default) ▪ [1] = R1.5 <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: User Defined Tone Enable [UserDefinedToneDetectorE]	Enables the detection of User Defined Tones signaling, applicable for Special Information Tone (SIT) detection. <ul style="list-style-type: none"> ▪ [0] = Disable (default)

Parameter	Description
nable]	<ul style="list-style-type: none"> ▪ [1] = Enable
EMS: SIT Enable [SITDetectorEnable]	<p>Enables SIT detection according to the ITU-T recommendation E.180/Q.35.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default). ▪ [1] = Enable. <p>To disconnect IP-to-ISDN calls when a SIT tone is detected, the following parameters must be configured:</p> <ul style="list-style-type: none"> ▪ SITDetectorEnable = 1 ▪ UserDefinedToneDetectorEnable = 1 ▪ ISDNDisconnectOnBusyTone = 1 (applicable for Busy, Reorder and SIT tones) <p>Another parameter for handling the SIT tone is SITQ850Cause, which determines the Q.850 cause value specified in the SIP Reason header that is included in a 4xx response when a SIT tone is detected on an IP-to-Tel call.</p> <p>To disconnect IP-to-CAS calls when a SIT tone is detected, the following parameters must be configured (applicable to FXO interfaces):</p> <ul style="list-style-type: none"> ▪ SITDetectorEnable = 1 ▪ UserDefinedToneDetectorEnable = 1 ▪ DisconnectOnBusyTone = 1 (applicable for Busy, Reorder and SIT tones) <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ The IP-to-ISDN call is disconnected on detection of a SIT tone only in call alert state. If the call is in connected state, the SIT does not disconnect the call. Detection of Busy or Reorder tones disconnect these calls also in call connected state. ▪ For IP-to-CAS calls, detection of Busy, Reorder, or SIT tones disconnect the call in any call state.
EMS: UDT Detector Frequency Deviation [UDTDetectorFrequencyDeviation]	<p>Defines the deviation (in Hz) allowed for the detection of each signal frequency.</p> <p>The valid range is 1 to 50. The default value is 50.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
EMS: CPT Detector Frequency Deviation [CPTDetectorFrequencyDeviation]	<p>Defines the deviation (in Hz) allowed for the detection of each CPT signal frequency.</p> <p>The valid range is 1 to 30. The default value is 10.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>

A.12.9.3 Metering Tone Parameters

The metering tone parameters are described in the table below.

Table A-63: 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. <ul style="list-style-type: none"> [0] Disable = Metering tones aren't generated (default). [1] Internal Table = Metering tones are generated according to the device's Charge Code table (using the ChargeCode parameter). Notes: <ul style="list-style-type: none"> This parameter is applicable only to FXS interfaces and ISDN Euro trunks for sending AOC Facility messages (see Advice of Charge Services for Euro ISDN on page 310). If you select 'Internal Table', you must configure the Charge Codes table (see Configuring Charge Codes Table on page 314).
Web: Analog Metering Type EMS: Metering Type [MeteringType]	Determines the metering method for generating pulses (sinusoidal metering burst frequency) by the FXS port. <ul style="list-style-type: none"> [0] 12 KHz (default) = 12 kHz sinusoidal bursts [1] 16 KHz = 16 kHz sinusoidal bursts [2] = Polarity Reversal pulses Notes: <ul style="list-style-type: none"> For this parameter to take effect, a device reset is required. This parameter is applicable only to FXS interfaces.
Web: Analog TTX Voltage Level EMS: TTX Voltage Level [AnalogTTXVoltageLevel]	Determines the metering signal/pulse voltage level (TTX). <ul style="list-style-type: none"> [0] 0V = 0 Vrms sinusoidal bursts [1] 0.5V = 0.5 Vrms sinusoidal bursts (default) [2] 1V = 1 Vrms sinusoidal bursts Notes: <ul style="list-style-type: none"> For this parameter to take effect, a device reset is required. This parameter is applicable only to FXS interfaces.
Charge Codes Table	
Web: Charge Codes Table EMS: Charge Codes [ChargeCode]	This <i>parameter</i> table configures metering tones and their time intervals that the device's FXS interface generates to the Tel side or the E1 trunk (EuroISDN) sends in AOC Facility messages to the PSTN (i.e., PBX). The format of this parameter is as follows: [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, <ul style="list-style-type: none"> EndTime = Period (1 - 4) end time. PulseInterval = Period (1 - 4) pulse interval. PulsesOnAnswer = Period (1 - 4) pulses on answer.

Parameter	Description
	<p>For example: ChargeCode 1 = 7,30,1,14,20,2,20,15,1,0,60,1; ChargeCode 2 = 5,60,1,14,20,1,0,60,1; ChargeCode 3 = 0,60,1; ChargeCode 0 = 6, 3, 1, 12, 2, 1, 18, 5, 2, 0, 2, 1;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The parameter can include up to 25 indices (i.e., up to 25 different metering rules can be defined). ▪ To associate a charge code to an outgoing Tel-to-IP call, use the Outbound IP Routing Table. ▪ To configure the Charge Codes table using the Web interface, see Configuring Charge Codes Table on page 314. ▪ For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.12.10 Telephone Keypad Sequence Parameters

The telephony keypad sequence parameters are described in the table below.

Table A-64: Keypad Sequence Parameters

Parameter	Description
Prefix for External Line	
[Prefix2ExtLine]	<p>Defines a string prefix (e.g., '9' dialed for an external line) that when dialed, the device plays a secondary dial tone (i.e., stutter tone) to the FXS line and then starts collecting the subsequently dialed digits from the FXS line.</p> <p>The valid range is a one-character string. The default is an empty string.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Determines whether the prefix string for accessing an external line (defined by the parameter Prefix2ExtLine) is added to the dialed number as the prefix and together sent to the IP destination (Tel-to-IP calls).</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable <p>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.</p> <p>Note: This parameter is applicable only to FXS interfaces.</p>

Parameter	Description
Hook Flash Parameters	
Web: Flash Keys Sequence Style [FlashKeysSequenceStyle]	Determines the hook-flash key sequence for FXS interfaces. <ul style="list-style-type: none"> ▪ [0] 0 = Flash hook (default) - only the phone's Flash button is used, according to the following scenarios: <ul style="list-style-type: none"> ✓ 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: <ul style="list-style-type: none"> ✓ 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: <ul style="list-style-type: none"> ✓ 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, and the device houses the MPM modules). Note that the settings of the ConferenceCode parameter are ignored. ✓ Flash + 4: makes a call transfer.
Web: Flash Keys Sequence Timeout [FlashKeysSequenceTimeout]	Defines the Flash keys sequence timeout - the time (in msec) that the device waits for digits after the user presses the Flash button (Flash Hook + Digit mode - when the parameter FlashKeysSequenceStyle is set to 1 or 2). 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]	Defines the keypad sequence to activate the immediate call forward option.
Web: No Answer EMS: Call Forward No Answer [KeyCFNoAnswer]	Defines the keypad sequence to activate the forward on no answer option.
Web: On Busy EMS: Call Forward Busy [KeyCFBusy]	Defines the keypad sequence to activate the forward on busy option.
Web: On Busy or No Answer EMS: CF Busy Or No Answer [KeyCFBusyOrNoAnswer]	Defines the keypad sequence to activate the forward on 'busy or no answer' option.

Parameter	Description
Web: Do Not Disturb EMS: CF Do Not Disturb [KeyCFDoNotDisturb]	Defines the keypad sequence to activate the Do Not Disturb option (immediately reject incoming calls).
To activate the required forward method from the telephone:	
<ol style="list-style-type: none"> 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]	Defines the keypad sequence to deactivate 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]	Defines the keypad sequence to activate the restricted Caller ID option. After the sequence is pressed, a confirmation tone is heard.
Web: Deactivate EMS: CLIR Deactivation [KeyCLIRDeact]	Defines the keypad sequence to deactivate 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]	Defines the keypad sequence to activate the delayed hotline option. To activate the delayed hotline option from the telephone, perform the following: <ol style="list-style-type: none"> 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]	Defines the keypad sequence to deactivate the delayed hotline option. After the sequence is pressed, a confirmation tone is heard.
Keypad Feature - Transfer Parameters	
Note: See the description of the KeyBlindTransfer parameter for this feature.	
Keypad Feature - Call Waiting Parameters	
Web: Activate EMS: Keypad Features CW [KeyCallWaiting]	Defines the keypad sequence to activate the Call Waiting option. After the sequence is pressed, a confirmation tone is heard.
Web: Deactivate EMS: Keypad Features CW Deact [KeyCallWaitingDeact]	Defines the keypad sequence to deactivate 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]	Defines the keypad sequence to activate the reject anonymous call option, whereby the device rejects incoming anonymous calls. After the sequence is pressed, a confirmation tone is heard.

Parameter	Description
Web: Deactivate EMS: Reject Anonymous Call Deact [KeyRejectAnonymousCallDeact]	Defines the keypad sequence that de-activate the reject anonymous call option. After the sequence is pressed, a confirmation tone is heard.
[RejectAnonymousCallPerPort]	This <i>parameter</i> table 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_Port, RejectAnonymousCallPerPort_Module; [\RejectAnonymousCallPerPort] Where, <ul style="list-style-type: none"> ▪ Enable = accept [0] (default) or reject [1] incoming anonymous calls. ▪ Port = Port number. ▪ Module = Module number. For example: RejectAnonymousCallPerPort 0 = 0,1,1; RejectAnonymousCallPerPort 1 = 1,2,1; If enabled, when a device's FXS interface receives an anonymous call, it responds with a 433 (Anonymity Disallowed) SIP response. Notes: <ul style="list-style-type: none"> ▪ This parameter is applicable only to FXS interfaces. ▪ This parameter is per FXS port. ▪ For configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.12.11 General FXO Parameters

The general FXO parameters are described in the table below.

Table A-65: 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. <ul style="list-style-type: none"> ▪ [66] Europe = TBR21 ▪ [70] USA = United States (default) Note: For this parameter to take effect, a device reset is required.
[FXODCTermination]	Defines the FXO line DC termination (i.e., resistance). <ul style="list-style-type: none"> ▪ [0] = DC termination is set to 50 Ohms (default). ▪ [1] = DC termination set to 800 Ohms. The termination changes from 50 to 800 Ohms only when moving from onhook to offhook. Note: For this parameter to take effect, a device reset is required.
[EnableFXOCurrentLimit]	Enables limiting the FXO loop current to a maximum of 60 mA (according to the TBR21 standard).

Parameter	Description
	<ul style="list-style-type: none"> ▪ [0] = FXO line current limit is disabled (default). ▪ [1] = FXO loop current is limited to a maximum of 60 mA. <p>Note: For this parameter to take effect, a device reset is required.</p>
[FXONumberOfRings]	<p>Defines the number of rings before the device's FXO interface answers a call by seizing the line. The valid range is 0 to 10. The default is 0.</p> <p>When set to 0, the FXO seizes the line after one ring. When set to 1, the FXO seizes the line after two rings.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Determines the dialing mode for IP-to-Tel (FXO) calls.</p> <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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]	<p>Determines whether the device waits for a dial tone before dialing the phone number for IP-to-Tel (FXO) calls.</p> <ul style="list-style-type: none"> ▪ [0] No = Don't wait for dial tone. ▪ [1] Yes = Wait for dial tone (default). <p>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.</p> <p>If this parameter is disabled, the device immediately dials the phone number after seizing the PSTN/PBX line without 'listening' for a dial tone.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 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.

Parameter	Description
Web: Time to Wait before Dialing [msec] EMS: Time Before Dial [WaitForDialTime]	<p>For digital interfaces: Defines the delay after hook-flash is generated and until dialing begins. Applies to call transfer (i.e., the parameter TrunkTransferMode is set to 3) on CAS protocols.</p> <p>For Analog interfaces: Defines the delay before the device starts dialing on the FXO line in the following scenarios:</p> <ul style="list-style-type: none"> ▪ 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. <p>The valid range (in milliseconds) is 0 to 20,000 (i.e., 20 seconds). The default value is 1,000 (i.e., 1 second).</p>
Web: Ring Detection Timeout [sec] EMS: Timeout Between Rings [FXOBetweenRingTime]	<p>Defines the timeout (in seconds) for detecting the second ring after the first detected ring.</p> <p>If automatic dialing is not used and Caller ID is enabled, the device seizes the line after detection of the second ring signal (allowing detection of caller ID sent between the first and the second rings). If the second ring signal is not received within this timeout, the device doesn't initiate a call to IP.</p> <p>If automatic dialing is used, the device initiates a call to IP when the ringing signal is detected. The FXO line is seized only if the remote IP party answers the call. If the remote party doesn't answer the call and the second ring signal is not received within this timeout, the device releases the IP call.</p> <p>This parameter is typically set to between 5 and 8. The default is 8.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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).
Web: Rings before Detecting Caller ID EMS: Rings Before Caller ID [RingsBeforeCallerID]	<p>Determines the number of rings before the device starts detecting Caller ID.</p> <ul style="list-style-type: none"> ▪ [0] 0 = Before first ring. ▪ [1] 1 = After first ring (default). ▪ [2] 2 = After second ring. <p>Note: This parameter is applicable only to FXO interfaces.</p>
Web/EMS: Guard Time Between Calls [GuardTimeBetweenCalls]	<p>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.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.

Parameter	Description
Web: FXO Double Answer [EnableFXODoubleAnswer]	Enables the FXO Double Answer feature, which rejects (disconnects) incoming Tel (FXO)-to-IP collect calls and signals (informs) this call denial to the PSTN. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable

A.12.12 FXS Parameters

The general FXS parameters are described in the table below.

Table A-66: 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. <ul style="list-style-type: none"> ▪ [66] Europe = TBR21 ▪ [70] USA = United States (default) <p>Note: For this parameter to take effect, a device reset is required.</p>

A.12.13 Trunk Groups and Routing Parameters

The routing parameters are described in the table below.

Table A-67: Routing Parameters

Parameter	Description
Trunk Group Table	
Web: Trunk Group Table EMS: SIP Endpoints > Phones [TrunkGroup]	<p>This <i>parameter</i> table is used to define and activate the device's endpoints/Trunk channels, by defining telephone numbers and assigning them to Trunk Groups. The format of this parameter is shown below:</p> <pre>[TrunkGroup] FORMAT TrunkGroup_Index = TrunkGroup_TrunkGroupNum, TrunkGroup_FirstTrunkId, TrunkGroup_FirstBChannel, TrunkGroup_LastBChannel, TrunkGroup_FirstPhoneNumber, TrunkGroup_ProfileId, TrunkGroup_LastTrunkId, TrunkGroup_Module; [\TrunkGroup]</pre> <p>For example, the configuration below assigns Trunk 1 (channels 1 to 30) of Module 1 to Trunk Group ID 2: TrunkGroup 0 = 2, 0, 1, 30, 50000, 0, 0, 1; the configuration below assigns BRI channels 1 through 4 of Module 2 to Trunk Group ID 2 with phone numbers 208 to 211: TrunkGroup 1 = 2, 0, 1, 4, 208, 0, 0 ,2;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The first entry in this table starts at index 0. ▪ Trunk Group ID 1 is depicted as 0 in the table. ▪ This parameter can appear up to four times per module.

Parameter	Description
	<ul style="list-style-type: none"> ▪ For configuring this table in the Web interface, see Configuring Trunk Group Table on page 249. ▪ For a description of <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Trunk Group Settings	
Web: Trunk Group Settings EMS: SIP Routing > Hunt Group [TrunkGroupSettings]	<p>This <i>parameter</i> table defines rules for channel allocation per Trunk Group. If no rule exists, the rule defined by the global parameter ChannelSelectMode takes effect. The format of this parameter is as follows:</p> <pre>[TrunkGroupSettings] FORMAT TrunkGroupSettings_Index = TrunkGroupSettings_TrunkGroupId, TrunkGroupSettings_ChannelSelectMode, TrunkGroupSettings_RegistrationMode, TrunkGroupSettings_GatewayName,TrunkGroupSettings_Contact User, TrunkGroupSettings_ServingIPGroup, TrunkGroupSettings_MWIInterrogationType; [TrunkGroupSettings]</pre> <p>Where,</p> <ul style="list-style-type: none"> ▪ MWIInterrogationType = defines QSIG MWI to IP interworking for interrogating MWI supplementary services: <ul style="list-style-type: none"> ✓ [255] Not Configured ✓ [0] None = disables the feature. ✓ [1] Use Activate Only = don't send any MWI Interrogation messages and only "passively" respond to MWI Activate requests from the PBX. ✓ [2] Result Not Used = send MWI Interrogation message, but don't use its result. Instead, wait for MWI Activate requests from the PBX. ✓ [3] Use Result = send MWI Interrogation messages, use its results, and use the MWI Activate requests. MWI Activate requests are interworked to SIP NOTIFY MWI messages. The SIP NOTIFY messages are sent to the IP Group defined by the NotificationIPGroupID parameter. <p>For example: TrunkGroupSettings 0 = 1, 0, 5, branch-hq, user, 1, 255; TrunkGroupSettings 1 = 2, 1, 0, localname, user1, 2, 255;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter can include up to 120 indices. ▪ For configuring Trunk Group Settings using the Web interface, see 'Configuring Trunk Group Settings' on page 251. ▪ For a description on using <i>ini</i> file table parameters, see to 'Configuring ini File Table Parameters' on page 84.
Web: Channel Select Mode EMS: Channel Selection Mode [ChannelSelectMode]	<p>Method for allocating incoming IP-to-Tel calls to a channel.</p> <ul style="list-style-type: none"> ▪ [0] By Dest Phone Number = Selects the channel according to the called (destination) number (default). If the number is not located, the call is released. If the channel is unavailable (e.g., busy), the call is put on call waiting (if call waiting is enabled and no other call is on call waiting); otherwise, the call is released. ▪ [1] Cyclic Ascending = Selects the next available channel (in the Trunk Group) in an ascending cyclic order. When the device reaches the highest channel number in the Trunk Group, it selects the lowest channel number in the Trunk Group and then

Parameter	Description
	<p>starts ascending again.</p> <ul style="list-style-type: none"> ▪ [2] Ascending = Selects the lowest available channel in the Trunk Group and if 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 Trunk Group. When the device reaches the lowest channel number in the Trunk Group, it selects the highest channel number in the Trunk Group and then starts descending again. ▪ [4] Descending = Selects the highest available channel in the Trunk Group and if 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. <p>Note: If the called number is located but the port associated with the number is busy, the call is released.</p> <ul style="list-style-type: none"> ▪ [6] By Source Phone Number = The device selects the channel according to the calling number. ▪ [7] Trunk Cyclic Ascending = The device selects the channel from the first channel of the next trunk (adjacent to the trunk from which the previous channel was allocated). This option is applicable only to digital interfaces. ▪ [8] Trunk & Channel Cyclic Ascending = The device implements the Trunk Cyclic Ascending and Cyclic Ascending methods to select the channel. This method selects the next physical trunk (pertaining to the Trunk Group) and then selects the B-channel of this trunk according to the cyclic ascending method (i.e., selects the channel after the last allocated channel). This option is applicable only to digital interfaces. <p>For example, if the Trunk Group includes two physical trunks, 0 and 1:</p> <ul style="list-style-type: none"> ✓ For the first incoming call, the first channel of Trunk 0 is allocated. ✓ For the second incoming call, the first channel of Trunk 1 is allocated. ✓ For the third incoming call, the second channel of Trunk 0 is allocated. <ul style="list-style-type: none"> ▪ [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 a call is received 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 (afterwhich the other phones stop ringing). This option is applicable only to FXS interfaces. ▪ [10] Select Trunk by ISDN SuppServ Table = The device selects the BRI port/module according to the settings in the ISDN Supplementary Services table (defined by the ISDN SuppServ parameter), allowing the routing of IP-to-Tel calls to specific BRI endpoints. ▪ [11] Dest Number + Ascending = The device allocates a channels to incoming IP-to-Tel calls as follows: <ul style="list-style-type: none"> a. The device attempts to route the call to the channel that is associated with the destination (called) number. If located,

Parameter	Description
	<p>the call is sent to that channel.</p> <ul style="list-style-type: none"> b. If the number is not located or the channel is unavailable (e.g., busy), the device searches, in ascending order, for the next available channel in the Trunk Group. If located, the call is sent to that channel. c. If the device all the channels are unavailable, the call is released. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For defining the channel select mode per Trunk Group, see 'Configuring Trunk Group Settings' on page 251. ▪ The logical (for digital interfaces) phone numbers of the device's B-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 Trunk Group Table' (see Configuring the Trunk Group Table on page 249). This parameter is used as a starting number for the list of channels comprising all the device's Trunk Groups. The default value is 1000.
Web: Source IP Address Input [SourceIPAddressInput]	Determines which IP address the device uses to determine the source of incoming INVITE messages for IP-to-Tel routing. <ul style="list-style-type: none"> ▪ [-1] = Auto Decision - if the IP-to-IP feature is enabled, this parameter is automatically set to Layer 3 Source IP. If the IP-to-IP feature is disabled, this parameter is automatically set to SIP Contact Header (1). (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 [UseSourceNumberAsDisplay Name]	Determines the use of Tel Source Number and Display Name for Tel-to-IP calls. <ul style="list-style-type: none"> ▪ [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. <ul style="list-style-type: none"> ▪ [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

Parameter	Description
	<p>received from IP, the IP Source Number is used as the Tel Source Number and Presentation is set to Restricted (1).</p> <p>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).</p> <p>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).</p>
<p>Web: Use Routing Table for Host Names and Profiles EMS: Use Routing Table For Host Names [AlwaysUseRouteTable]</p>	<p>Determines whether to use the device's routing table to obtain the URI host name and optionally, an IP profile (per call) even if a Proxy server is used.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Don't use internal routing table (default). ▪ [1] Enable = Use the Outbound IP Routing Table'. <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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.
<p>Web/EMS: Tel to IP Routing Mode [RouteModeTel2IP]</p>	<p>For a description of this parameter, see 'Configuring Outbound IP Routing Table' on page 269.</p>
Outbound IP Routing Table	
<p>Web: Outbound IP Routing Table EMS: SIP Routing > Tel to IP [Prefix]</p>	<p>This <i>parameter</i> table configures the Outbound IP Routing Table' for routing Tel-to-IP and IP-to-IP calls. The format of this parameter is as follows:</p> <p>[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_CostGroup, PREFIX_ForkingGroup; [\PREFIX]</p> <p>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,;;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter can include up to 200 indices. ▪ For a detailed description of the table's parameters and for configuring this table using the Web interface, see 'Configuring Outbound IP Routing Table' on page 269. ▪ For a description on using <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Inbound IP Routing Table	
<p>Web: Inbound IP Routing Table EMS: SIP Routing > IP to Hunt [PSTNPrefix]</p>	<p>This <i>parameter</i> table configures the routing of IP calls to Trunk Groups (or inbound IP Groups). The format of this parameter is as follows:</p> <p>[PSTNPrefix] FORMAT PstnPrefix_Index = PstnPrefix_DestPrefix,</p>

Parameter	Description
	<p>PstnPrefix_TrunkGroupId, PstnPrefix_SourcePrefix, PstnPrefix_SourceAddress, PstnPrefix_ProfileId, PstnPrefix_SrcIPGroupId, PstnPrefix_DestHostPrefix, PstnPrefix_SrcHostPrefix; [PSTNPrefix]</p> <p>For example: PstnPrefix 0 = 100, 1, 200, *, 0, 2, , ; PstnPrefix 1 = *, 2, *, , 1, 3, acl, joe;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter can include up to 24 indices. ▪ For a description of the table's parameters, refer to the corresponding Web parameters in 'Configuring Inbound IP Routing Table' on page 277. ▪ To support the In-Call Alternative Routing feature, you can use two entries that support the same call but assigned with a different Trunk 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 Trunk 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 767. ▪ For a description on using <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Web/EMS: IP to Tel Routing Mode [RouteModeIP2Tel]	<p>Determines whether to route IP calls to the Trunk Group (or IP Group) before or after manipulation of the destination number (configured in 'Configuring Number Manipulation Tables' on page 254).</p> <ul style="list-style-type: none"> ▪ [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.
Web: IP Security EMS: Secure Call From IP [SecureCallsFromIP]	<p>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.</p> <ul style="list-style-type: none"> ▪ [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 Outbound IP Routing Table' or Proxy Set table, or IP addresses resolved from DNS servers from FQDN values defined in the Proxy Set table. All other incoming calls are rejected.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [2] Secure All calls = The device accepts SIP calls only from IP addresses (in dotted-decimal notation format) that are defined in the Outbound IP Routing Table table or Proxy Set table, and rejects all other incoming calls. In addition, if an FQDN is defined in the routing table or Proxy Set table, the call is allowed to be sent only if the resolved DNS IP address appears in one of these tables; otherwise, the call is rejected. Therefore, the difference between this option and option [1] is that this option is concerned only about numerical IP addresses that are defined in the tables. <p>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.</p>
Web/EMS: Filter Calls to IP [FilterCalls2IP]	<p>Enables filtering of Tel-to-IP calls when a Proxy is used (i.e., IsProxyUsed parameter is set to 1 - see 'Configuring Proxy and Registration Parameters' on page 226).</p> <ul style="list-style-type: none"> ▪ [0] Don't Filter = device doesn't filter calls when using a Proxy (default). ▪ [1] Filter = Filtering is enabled. <p>When this parameter is enabled and a Proxy is used, the device first checks the Outbound IP Routing Table' before making a call through the Proxy. If the number is not allowed (i.e., number isn't listed in the table or a call restriction routing rule of IP address 0.0.0.0 is applied), the call is released.</p> <p>Note: When no Proxy is used, this parameter must be disabled and filtering is according to the Outbound IP Routing Table'.</p>
[IP2TelTaggingDestDialPlanIndex]	<p>Determines the Dial Plan index in the external Dial Plan file (.dat) in which string labels ("tags") are defined for tagging incoming IP-to-Tel calls. The special "tag" is added as a prefix to the called party number, and then the Inbound IP Routing Table' uses this "tag" instead of the original prefix. Manipulation is then performed (after routing) in the Manipulation table which strips the "tag" characters before sending the call to the endpoint.</p> <p>The valid values are 0 to 7, where 0 denotes PLAN1, 1 denotes PLAN2, and so on. The default is -1 (i.e., no dial plan file used). The routing label can be up to 9 (text) characters.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only to digital interfaces. ▪ The routing must be configured to be performed before manipulation. ▪ For more information on this feature, see Dial Plan Prefix Tags for IP-to-Tel Routing on page 338.
[EnableETSIDiversion]	<p>Determines the method in which the Redirect Number is sent to the Tel side.</p> <ul style="list-style-type: none"> ▪ [0] = Q.931 Redirecting Number Information Element (IE) (default) ▪ [1] = ETSI DivertingLegInformation2 in a Facility IE
Web: Add CIC [AddCicAsPrefix]	<p>Determines whether to add the Carrier Identification Code (CIC) as a prefix to the destination phone number for IP-to-Tel calls.</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ [0] No (default) ▪ [1] Yes <p>When this parameter is enabled, the cic parameter in the incoming SIP INVITE can be used for IP-to-Tel routing decisions. It routes the call to the appropriate Trunk Group based on this parameter's value.</p> <p>The SIP cic parameter enables the transmission of the cic parameter from the SIP network to the ISDN. The cic parameter is a three- or four-digit code used in routing tables to identify the network that serves the remote user when a call is routed over many different networks. The cic parameter is carried in the SIP INVITE and maps to the ISDN Transit Network Selection Information Element (TNS IE) in the outgoing ISDN Setup message (if the EnableCIC parameter is set to 1). The TNS IE identifies the requested transportation networks and allows different providers equal access support, based on customer choice.</p> <p>For example, as a result of receiving the below INVITE, the destination number after number manipulation is cic+167895550001: INVITE sip:5550001;cic=+16789@172.18.202.60:5060;user=phone SIP/2.0</p> <p>Note: After the cic prefix is added, the Inbound IP Routing Table' can be used to route this call to a specific Trunk Group. The Destination Number IP to Tel Manipulation table must be used to remove this prefix before placing the call to the ISDN.</p>

A.12.14 Alternative Routing Parameters

The alternative routing parameters are described in the table below.

Table A-68: Alternative Routing Parameters

Parameter	Description
Web/EMS: Redundant Routing Mode [RedundantRoutingMode]	<p>Determines the type of redundant routing mechanism when a call can't be completed using the main route.</p> <ul style="list-style-type: none"> ▪ [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. <p>Note: To implement the Redundant Routing Mode mechanism, you first need to configure the parameter AltRouteCauseTEL2IP (Reasons for Alternative Routing table).</p>
Web: Enable Alt Routing Tel to IP EMS: Enable Alternative Routing [AltRoutingTel2IPEnable]	<p>Enables the Alternative Routing feature for Tel-to-IP calls.</p> <ul style="list-style-type: none"> ▪ [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

Parameter	Description
	<p>destination IP addresses is provided.</p> <p>For information on the Alternative Routing feature, see 'Configuring Alternative Routing (Based on Connectivity and QoS)' on page 340.</p>
<p>Web: Alt Routing Tel to IP Mode EMS: Alternative Routing Mode [AltRoutingTel2IPMode]</p>	<p>Determines the event(s) reason for triggering Alternative Routing.</p> <ul style="list-style-type: none"> ▪ [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). <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 'Configuring Alternative Routing (Based on Connectivity and QoS)' on page 340. ▪ To receive quality information (displayed in the 'Quality Status' and 'Quality Info.' fields in 'Viewing IP Connectivity' on page 510) per destination, this parameter must be set to 2 or 3.
<p>Web: Alt Routing Tel to IP Connectivity Method EMS: Alternative Routing Telephone to IP Connection Method [AltRoutingTel2IPConnMethod]</p>	<p>Determines the method used by the device for periodically querying the connectivity status of a destination IP address.</p> <ul style="list-style-type: none"> ▪ [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.
<p>[EnableAltMapTel2IP]</p>	<p>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).</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable
<p>Web: Alt Routing Tel to IP Keep Alive Time EMS: Alternative Routing Keep Alive Time [AltRoutingTel2IPKeepAliveTime]</p>	<p>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.</p>

Parameter	Description
Web/EMS: Alternative Routing Tone Duration [ms] [AltRoutingToneDuration]	Defines 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]	Defines the 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]	Defines the transmission delay (in msec) at which the IP connection is considered a failure and the Alternative Routing mechanism is activated. The range is 100 to 10,000. The default value is 250.
Reasons for Alternative Tel-to-IP Routing Table	
Web: Reasons for Alternative Routing EMS: Alt Route Cause Tel to IP [AltRouteCauseTel2IP]	<p>This <i>parameter</i> table 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 'Outbound IP Routing Table' (if a Proxy is not used) or used as a redundant Proxy (you need to set the parameter RedundantRoutingMode to 2). The release reason for Tel-to-IP calls is provided in SIP 4xx, 5xx, and 6xx response codes.</p> <p>The format of this parameter is as follows: [AltRouteCauseTel2IP] FORMAT AltRouteCauseTel2IP_Index = AltRouteCauseTel2IP_ReleaseCause; [AltRouteCauseTel2IP]</p> <p>For example: AltRouteCauseTel2IP 0 = 486; (Busy Here) AltRouteCauseTel2IP 1 = 480; (Temporarily Unavailable) AltRouteCauseTel2IP 2 = 408; (No Response)</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84
Reasons for Alternative IP-to-Tel Routing Table	
Web: Reasons for Alternative IP-to-Tel Routing	This <i>parameter</i> table configures call failure reason values received from the PSTN side (in Q.931 presentation). If a call is

Parameter	Description
EMS: Alt Route Cause IP to Tel [AltRouteCauseIP2Tel]	<p>released as a result of one of these reasons, the device attempts to locate an alternative Trunk Group for the call in the Inbound IP Routing Table'.</p> <p>The format of this parameter is as follows:</p> <pre>[AltRouteCauseIP2Tel] FORMAT AltRouteCauseIP2Tel_Index = AltRouteCauseIP2Tel_ReleaseCause; [AltRouteCauseIP2Tel]</pre> <p>For example:</p> <pre>AltRouteCauseIP2Tel 0 = 3 (No Route to Destination) AltRouteCauseIP2Tel 1 = 1 (Unallocated Number) AltRouteCauseIP2Tel 2 = 17 (Busy Here) AltRouteCauseIP2Tel 2 = 27 (Destination Out of Order)</pre> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter can include up to 5 indices. ▪ If the device fails to establish a call to the PSTN because it has no available channels in a specific Trunk Group (e.g., all the channels are occupied, or the spans are disconnected or out-of-sync), it uses the Internal Release Cause '3' (No Route to Destination). This cause can be used in the AltRouteCauseIP2Tel table to define routing to an alternative Trunk Group. ▪ 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 configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Forward On Busy Trunk Destination Table	
Web/EMS: Forward On Busy Trunk Destination [ForwardOnBusyTrunkDest]	<p>This parameter table configures the Forward On Busy Trunk Destination table. This table allows you to define an alternative IP destination if a trunk is busy, for IP-to-Tel calls. The destination can be an IP address or a SIP Request-URI user name and host part (i.e., user@host).</p> <p>The format of this parameter is as follows:</p> <pre>[ForwardOnBusyTrunkDest] FORMAT ForwardOnBusyTrunkDest_Index = ForwardOnBusyTrunkDest_TrunkGroupId, ForwardOnBusyTrunkDest_ForwardDestination; [ForwardOnBusyTrunkDest]</pre> <p>For example, the below configuration forwards IP-to-Tel calls to destination user "112" at host IP address 10.13.4.12, port 5060, using transport protocol TCP, if Trunk Group ID 2 is unavailable:</p> <pre>ForwardOnBusyTrunkDest 1 = 2, 112@10.13.4.12:5060;transport=tcp;</pre> <p>When configured with user@host, the original destination number is replaced by the user part.</p>

Parameter	Description
	<p>Notes:</p> <ul style="list-style-type: none"> The maximum number of indices (starting from 1) depends on the maximum number of Trunk 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 more information, see Configuring Call Forward upon Busy Trunk on page 281

A.12.15 Number Manipulation Parameters

The number manipulation parameters are described in the table below.

Table A-69: Number Manipulation Parameters

Parameter	Description
Use EndPoint Number As Calling Number Tel2IP [UseEPNumAsCallingNumTel2IP]	Enables the use of the B-channel number as the calling number (sent in the From field of the INVITE) instead of the number received in the Q.931 Setup message, for Tel-to-IP calls. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable For example, if the incoming calling party number in the Q.931 Setup message is "12345" and the B-channel number is 17, then the outgoing INVITE From header is set to "17" instead of "12345". <p>Note: When enabled, this feature is applied before routing and manipulation on the source number.</p>
Use EndPoint Number As Calling Number IP2Tel [UseEPNumAsCallingNumIP2Tel]	Enables the use of the B-channel number as the calling party number (sent in the Q.931 Setup message) instead of the number received in the From header of the INVITE, for IP-to-Tel calls. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable For example, if the incoming INVITE From header contains "12345" and the destined B-channel number is 17, then the outgoing calling party number in the Q.931 Setup message is set to "17" instead of "12345". <p>Note: When enabled, this feature is applied after routing and manipulation on the source number (i.e., just before sending to the Tel side).</p>

Parameter	Description
Web: Tel2IP Default Redirect Reason [Tel2IPDefaultRedirectReason]	Determines the default redirect reason for Tel-to-IP calls when no redirect reason (or “unknown”) exists in the received Q931 ISDN Setup message. The device includes this default redirect reason in the SIP History-Info header of the outgoing INVITE. If a redirect reason exists in the received Setup message, this parameter is ignored and the device sends the INVITE message with the reason according to the received Setup message. If this parameter is not configured (-1), the outgoing INVITE is sent with the redirect reason as received in the Setup message (if none or “unknown” reason, then without a reason). <ul style="list-style-type: none"> ▪ [-1] Not Configured (default) = Received redirect reason is not changed ▪ [1] Busy = Call forwarding busy ▪ [2] No Reply = Call forwarding no reply ▪ [9] DTE Out of Order = Call forwarding DTE out of order ▪ [10] Deflection = Call deflection ▪ [15] Systematic/Unconditional = Call forward unconditional
Web: Set Redirect number Screening Indicator to TEL EMS: Set IP To Tel Redirect Screening Indicator [SetIp2TelRedirectScreeningInd]	Determines the value of the Redirect Number screening indicator in ISDN Setup messages. <ul style="list-style-type: none"> ▪ [-1] Not Configured (default) ▪ [0] User Provided ▪ [1] User Passed ▪ [2] User Failed ▪ [3] Network Provided Note: This parameter is applicable only to digital PSTN interfaces (ISDN).
Web: Set IP-to-TEL Redirect Reason [SetIp2TelRedirectReason]	Defines the redirect reason for IP-to-Tel calls. If redirect (diversion) information is received from the IP, the redirect reason is set to the value of this parameter before the device sends it on to the Tel. <ul style="list-style-type: none"> ▪ [-1] Not Configured (default) ▪ [0] Unkown ▪ [1] Busy ▪ [2] No Reply ▪ [3] Network Busy ▪ [4] Deflection ▪ [9] DTE out of Order ▪ [10] Forwarding DTE ▪ [13] Transfer ▪ [14] Pickup ▪ [15] Systematic/Unconditional Note: This parameter is applicable only to digital PSTN interfaces (ISDN).

Parameter	Description
Web: Set TEL-to-IP Redirect Reason [SetTel2IpRedirectReason]	Defines the redirect reason for Tel-to-IP calls. If redirect (diversion) information is received from the Tel, the redirect reason is set to the value of this parameter before the device sends it on to the IP. <ul style="list-style-type: none"> ▪ [-1] Not Configured (default) ▪ [0] Unkown ▪ [1] Busy ▪ [2] No Reply ▪ [3] Network Busy ▪ [4] Deflection ▪ [9] DTE out of Order ▪ [10] Forwarding DTE ▪ [13] Transfer ▪ [14] Pickup ▪ [15] Systematic/Unconditional Note: This parameter is applicable only to digital PSTN interfaces (ISDN).
Web: Send Screening Indicator to IP EMS: Screening Indicator To IP [ScreeningInd2IP]	Overrides the calling party's number (CPN) screening indication in the received ISDN SETUP message for Tel-to-IP calls. <ul style="list-style-type: none"> ▪ [-1] Not Configured = not configured (interworking from ISDN to IP) or set to 0 for CAS (default). ▪ [0] User Provided = CPN set by user, but not screened (verified). ▪ [1] User Passed = CPN set by user, verified and passed. ▪ [2] User Failed = CPN set by user, and verification failed. ▪ [3] Network Provided = CPN set by network. Note: This parameter is applicable only if the Remote Party ID (RPID) header is enabled.
Web: Send Screening Indicator to ISDN EMS: Screening Indicator To ISDN [ScreeningInd2ISDN]	Overrides the screening indicator of the calling party's number for IP-to-Tel ISDN calls. <ul style="list-style-type: none"> ▪ [-1] Not Configured = Not configured (interworking from IP to ISDN) (default). ▪ [0] User Provided = user provided, not screened. ▪ [1] User Passed = user provided, verified and passed. ▪ [2] User Failed = user provided, verified and failed. ▪ [3] Network Provided = network provided Note: This parameter is applicable only to digital PSTN interfaces (ISDN).

Parameter	Description
Web: Copy Destination Number to Redirect Number EMS: Copy Dest to Redirect Number [CopyDest2RedirectNumber]	<p>Determines whether the device copies the received ISDN (digital interfaces) called number to the outgoing SIP Diversion header for Tel-to-IP calls (even if a Redirecting Number IE is not received in the ISDN Setup message, for digital interfaces). Therefore, the called number is used as a redirect number. Call redirection information is typically used for Unified Messaging and voice mail services to identify the recipient of a message.</p> <ul style="list-style-type: none"> ▪ [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. <p>Notes:</p> <ul style="list-style-type: none"> ▪ For digital interfaces: If the incoming ISDN-to-IP call includes a Redirect Number, this number is overridden by the new called number if this parameter is set to [1] or [2]. ▪ When configured in an IP Profile, this parameter can also be used for IP-to-Tel calls. The device can overwrite the redirect number with the destination number from the received SIP INVITE message in the outgoing ISDN call. This is achieved by assigning an IP Profile (IPProfile parameter) defined with the CopyDest2RedirectNumber parameter set to 1, to the IP-to-Tel Routing table (PSTNPrefix parameter). Even if there is no SIP Diversion or History header in the incoming INVITE message, the outgoing Q.931 Setup message will contain a redirect number. ▪ This parameter can also be configured per IP Profile (using the IPProfile parameter).
[ReplaceCallingWithRedirectNumber]	<p>Enables replacing the calling number with the redirect number in ISDN-to-IP calls. When such a replacement occurs, the calling name is deleted and left blank. The outgoing INVITE message does not include the redirect number that was used to replace the calling number. The replacement is done only if a redirect number is present in the incoming call.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable
Web/EMS: Add Trunk Group ID as Prefix [AddTrunkGroupAsPrefix]	<p>Determines whether the Trunk Group ID is added as a prefix to the destination phone number (i.e., called number) for Tel-to-IP calls.</p> <ul style="list-style-type: none"> ▪ [0] No = Don't add Trunk Group ID as prefix (default). ▪ [1] Yes = Add Trunk Group ID as prefix to called number. <p>Notes:</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ This option can be used to define various routing rules. ▪ To use this feature, you must configure the Trunk Group IDs (see Configuring Trunk Group Table on page 249).
Web: Add Trunk ID as Prefix EMS: Add Port ID As Prefix [AddPortAsPrefix]	Determines whether the port number / Trunk ID is added as a prefix to the called number for Tel-to-IP calls. <ul style="list-style-type: none"> ▪ [0] No = port number / Trunk ID not added as prefix (default). ▪ [1] Yes = port number / Trunk ID added as prefix If enabled, the slot number (a single digit in the range of 1 to 6) and port number/Trunk ID (single digit in the range 1 to 8) are added as a prefix to the called (destination) phone number. For example, for the first trunk/channel located in the first slot, the number "11" is added as the prefix. 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 Trunk Group ID (from where the call originated) as the prefix to the calling number (i.e. source number). <ul style="list-style-type: none"> ▪ [0] No (default) ▪ [1] Yes
Web: Replace Empty Destination with B-channel Phone Number EMS: Replace Empty Dst With Port Number [ReplaceEmptyDstWithPortNumber]	Determines whether the internal channel number is used as the destination number if the called number is missing. <ul style="list-style-type: none"> ▪ [0] No (default) ▪ [1] Yes Note: This parameter is applicable only to Tel-to-IP calls and if the called number is missing.
[CopyDestOnEmptySource]	<ul style="list-style-type: none"> ▪ [0] = Leave Source Number empty (default). ▪ [1] = If the Source Number of a Tel-to-IP call is empty, the Destination Number is copied to the Source Number.
Web: Add NPI and TON to Calling Number EMS: Add NPI And TON As Prefix To Calling Number [AddNPIandTON2CallingNumber]	Determines whether the Numbering Plan Indicator (NPI) and Type of Numbering (TON) are added to the Calling Number for Tel-to-IP calls. <ul style="list-style-type: none"> ▪ [0] No = Do not change the Calling Number (default). ▪ [1] Yes = Add NPI and TON to the Calling Number ISDN Tel-to-IP call. For example: After receiving a Calling Number of 555, NPI of 1, and TON of 3, the modified number becomes 13555. This number can later be used for manipulation and routing.
Web: Add NPI and TON to Called Number EMS: Add NPI And TON As Prefix To Called Number [AddNPIandTON2CalledNumber]	Determines whether NPI and TON are added to the Called Number for Tel-to-IP calls. <ul style="list-style-type: none"> ▪ [0] No = Do not change the Called Number (default). ▪ [1] Yes = Add NPI and TON to the Called Number of ISDN Tel-to-IP call. For example: After receiving a Called Number of 555, NPI of 1 and TON of 3, the modified number becomes 13555. This number can later be used for manipulation and routing.
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. <ul style="list-style-type: none"> ▪ [0] No = Don't remove prefix (default) ▪ [1] Yes = Remove the prefix (defined in the Inbound IP Routing Table' - see 'Configuring Inbound IP Routing Table')

Parameter	Description
	<p>on page 277) from a telephone number for an IP-to-Tel call before forwarding it to Tel.</p> <p>For example: To route an incoming IP-to-Tel call with destination number 21100, the Inbound IP Routing Table' is scanned for a matching prefix. If such a prefix is found (e.g., 21), then before the call is routed to the corresponding Trunk Group, the prefix (21) is removed from the original number, and therefore, only 100 remains.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter is applicable only if number manipulation is performed after call routing for IP-to-Tel calls (i.e., RouteModelIP2Tel parameter is set to 0). ▪ Similar operation (of removing the prefix) is also achieved by using the usual number manipulation rules.
Web/EMS: Swap Redirect and Called Numbers [SwapRedirectNumber]	<ul style="list-style-type: none"> ▪ [0] No = Don't change numbers (default). ▪ [1] Yes = Incoming ISDN call that includes a redirect number (sometimes referred to as 'original called number') uses the redirect number instead of the called number.
[SwapTel2IPCalled&CallingNumbers]	<p>Determines whether the device swaps the calling and called numbers received from the Tel side (for Tel-to-IP calls). The SIP INVITE message contains the swapped numbers.</p> <ul style="list-style-type: none"> ▪ [0] = Disabled (default) ▪ [1] = Swap calling and called numbers <p>Note: This parameter can also be configured per Tel Profile, using the TelProfile parameter.</p>
Web/EMS: Add Prefix to Redirect Number [Prefix2RedirectNumber]	<p>Defines a string prefix that is added to the Redirect number received from the Tel side. This prefix is added to the Redirect Number in the SIP Diversion header.</p> <p>The valid range is an 8-character string. The default is an empty string.</p>
Web: Add Number Plan and Type to RPI Header EMS: Add Ton 2 RPI [AddTON2RPI]	<p>Determines whether the TON/PLAN parameters are included in the Remote-Party-ID (RPID) header.</p> <ul style="list-style-type: none"> ▪ [0] No ▪ [1] Yes (default) <p>If the Remote-Party-ID header is enabled (EnableRPIHeader = 1) and AddTON2RPI = 1, it's possible to configure the calling and called number type and number plan using the Number Manipulation tables for Tel-to-IP calls.</p>
Web/EMS: Source Manipulation Mode [SourceManipulationMode]	<p>Determines the SIP headers containing the source number after manipulation:</p> <ul style="list-style-type: none"> ▪ [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.
Calling Name Manipulations IP-to-Tel Table	
[CallingNameMapIp2Tel]	<p>Configures rules for manipulating the calling name (caller ID) in the received SIP message for IP-to-Tel calls. This can include modifying or removing the calling name. The format of this ini</p>

Parameter	Description
	file parameter table is as follows: [CallingNameMapIp2Tel] FORMAT CallingNameMapIp2Tel_Index = CallingNameMapIp2Tel_DestinationPrefix, CallingNameMapIp2Tel_SourcePrefix, CallingNameMapIp2Tel_CallingNamePrefix, CallingNameMapIp2Tel_SourceAddress, CallingNameMapIp2Tel_RemoveFromLeft, CallingNameMapIp2Tel_RemoveFromRight, CallingNameMapIp2Tel_LeaveFromRight, CallingNameMapIp2Tel_Prefix2Add, CallingNameMapIp2Tel_Suffix2Add; [\CallingNameMapIp2Tel]
Calling Name Manipulations Tel-to-IP Table	
[CallingNameMapTel2Ip]	Configures rules for manipulating the calling name (caller ID) for Tel-to-IP calls. This can include modifying or removing the calling name. [CallingNameMapTel2Ip] FORMAT CallingNameMapTel2Ip_Index = CallingNameMapTel2Ip_DestinationPrefix, CallingNameMapTel2Ip_SourcePrefix, CallingNameMapTel2Ip_CallingNamePrefix, CallingNameMapTel2Ip_SrcTrunkGroupID, CallingNameMapTel2Ip_SrcIPGroupID, CallingNameMapTel2Ip_RemoveFromLeft, CallingNameMapTel2Ip_RemoveFromRight, CallingNameMapTel2Ip_LeaveFromRight, CallingNameMapTel2Ip_Prefix2Add, CallingNameMapTel2Ip_Suffix2Add; [\CallingNameMapTel2Ip]
Destination Phone Number Manipulation for IP-to-Tel Calls Table	
Web: Destination Phone Number Manipulation Table for IP > Tel Calls EMS: EMS: SIP Manipulations > Destination IP to Telcom [NumberMapIP2Tel]	This <i>parameter</i> table 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 = 01,034,10.13.77.8,\$\$,0,\$\$,2,\$\$,667,\$\$; NumberMapIp2Tel 1 = 10,10,1.1.1.1,255,255,3,0,5,100,\$\$,255; Notes: <ul style="list-style-type: none"> ▪ This table parameter can include up to 100 indices. ▪ The manipulation rules are done in the following order:

Parameter	Description
	<p>RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and then Suffix2Add.</p> <ul style="list-style-type: none"> ▪ If the called and calling numbers match the DestinationPrefix, SourcePrefix, and/or SourceAddress conditions, then the RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, LeaveFromRight, NumberType, and/or NumberPlan are applied. ▪ The Source IP address can include the following wildcards: <ul style="list-style-type: none"> ✓ '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 parameter is not applicable: IsPresentationRestricted. ▪ To configure manipulation of destination numbers for IP-to-Tel calls using the Web interface, see 'Configuring Number Manipulation Tables' on page 254). ▪ For a description on using <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
[PerformAdditionalIP2TELDestinationManipulation]	<p>Enables additional destination number manipulation for IP-to-Tel calls. The additional manipulation is done on the initially manipulated destination number, and this additional rule is also configured in the manipulation table (NumberMapIP2Tel parameter). This enables you to configure only a few manipulation rules for complex number manipulation requirements (that generally require many rules).</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable
Destination Phone Number Manipulation for Tel-to-IP Calls Table	
<p>Web: Destination Phone Number Manipulation Table for Tel > IP Calls EMS: SIP Manipulations > Destination Telcom to IPs [NumberMapTel2IP]</p>	<p>This <i>parameter</i> table manipulates the destination number of Tel-to-IP calls. The format of this parameter is as follows:</p> <pre>[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]</pre> <p>For example: NumberMapTel2Ip 0 = 01,\$\$,*,0,0,2,\$\$, \$\$,971,\$\$, \$\$,\$\$, \$\$; NumberMapTel2Ip 1 = 10,10,*,255,255,3,0,5,100,\$\$,255,\$\$, \$\$;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table parameter can include up to 120 indices (0-119).

Parameter	Description
	<ul style="list-style-type: none"> ▪ 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 NumberType, NumberPlan, RemoveFromLeft, RemoveFromRight, Prefix2Add, Suffix2Add, and/or LeaveFromRight are applied. ▪ Number Plan and Type can be used in the Remote-Party-ID header by configuring the EnableRPIHeader and AddTON2RPI parameters. ▪ The following parameters are not applicable: 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 254). ▪ For a description on using <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Source Phone Number Manipulation for IP-to-Tel Calls Table	
<p>Web: Source Phone Number Manipulation Table for IP > Tel Calls EMS: EMS: SIP Manipulations > Source IP to Telecom [SourceNumberMapIP2Tel]</p>	<p>This <i>parameter</i> table manipulates the source number for IP-to-Tel calls. The format of this parameter is as follows:</p> <pre>[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]</pre> <p>For example: SourceNumberMapIp2Tel 0 = 22,03,\$\$, \$\$, \$\$, \$\$, 2,667,\$\$, \$\$; SourceNumberMapIp2Tel 1 = 034,01,1.1.1.1,\$\$,0,2,\$\$, \$\$,972,\$\$,10;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table parameter can include up to 120 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, LeaveFromRight, NumberType, and/or NumberPlan are applied. <ul style="list-style-type: none"> ✓ '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.

Parameter	Description
	<ul style="list-style-type: none"> ▪ To configure manipulation of source numbers for IP-to-Tel calls using the Web interface, see 'Configuring Number Manipulation Tables' on page 254). ▪ For a description on using <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
[PerformAdditionalIP2TELSourceManipulation]	<p>Enables additional source number manipulation for IP-to-Tel calls. The additional manipulation is done on the initially manipulated source number, and this additional rule is also configured in the manipulation table (SourceNumberMapIP2Tel parameter). This enables you to configure only a few manipulation rules for complex number manipulation requirements (that generally require many rules).</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable
Source Phone Number Manipulation for Tel-to-IP Calls Table	
<p>Web: Source Phone Number Manipulation Table for Tel > IP Calls EMS: SIP Manipulations > Source Telcom to IP [SourceNumberMapTel2IP]</p>	<p>This <i>parameter</i> table manipulates the source phone number for Tel-to-IP calls. The format of this parameter is as follows:</p> <p>[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]</p> <p>For example: SourceNumberMapTel2Ip 0 = 22,03,\$\$,0,0,\$\$,2,\$\$,667,\$\$,0,\$\$,\$\$; SourceNumberMapTel2Ip 0 = 10,10,* ,255,255,3,0,5,100,\$\$,255,\$\$,\$\$;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ This table parameter can include up to 120 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'. ▪ Number Plan and Type can optionally be used in the Remote

Parameter	Description
	Party ID header by configuring the EnableRPIHeader and AddTON2RPI parameters. <ul style="list-style-type: none"> ▪ To configure manipulation of source numbers for Tel-to-IP calls using the Web interface, see 'Configuring Number Manipulation Tables' on page 254). ▪ For a description on using <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
<p>For the ETSI ISDN variant, the following Number Plan and Type combinations (Plan/Type) are supported in the Destination and Source Manipulation tables:</p> <ul style="list-style-type: none"> ▪ 0,0 = Unknown, Unknown ▪ 9,0 = Private, Unknown ▪ 9,1 = Private, Level 2 Regional ▪ 9,2 = Private, Level 1 Regional ▪ 9,3 = Private, PISN Specific ▪ 9,4 = Private, Level 0 Regional (local) ▪ 1,0 = Public(ISDN/E.164), Unknown ▪ 1,1 = Public(ISDN/E.164), International ▪ 1,2 = Public(ISDN/E.164), National ▪ 1,3 = Public(ISDN/E.164), Network Specific ▪ 1,4 = Public(ISDN/E.164), Subscriber ▪ 1,6 = Public(ISDN/E.164), Abbreviated <p>For the NI-2 and DMS-100 ISDN variants, the valid combinations of TON and NPI for calling and called numbers are (Plan/Type):</p> <ul style="list-style-type: none"> ▪ 0/0 - Unknown/Unknown ▪ 1/1 - International number in ISDN/Telephony numbering plan ▪ 1/2 - National number in ISDN/Telephony numbering plan ▪ 1/4 - Subscriber (local) number in ISDN/Telephony numbering plan ▪ 9/4 - Subscriber (local) number in Private numbering plan 	
<p>Redirect Number IP -to-Tel Table</p>	
Web: Redirect Number IP -> Tel EMS: Redirect Number Map IP to Tel [RedirectNumberMapIp2Tel]	This parameter table manipulates the redirect number for IP-to-Tel calls. This manipulates the value of the SIP Diversion, History-Info, or Resource-Priority headers (including the reason the call was redirected). The format of this parameter is as follows: [RedirectNumberMapIp2Tel] FORMAT RedirectNumberMapIp2Tel_Index = RedirectNumberMapIp2Tel_DestinationPrefix, RedirectNumberMapIp2Tel_RedirectPrefix, RedirectNumberMapIp2Tel_SourceAddress, RedirectNumberMapIp2Tel_NumberType, RedirectNumberMapIp2Tel_NumberPlan, RedirectNumberMapIp2Tel_RemoveFromLeft, RedirectNumberMapIp2Tel_RemoveFromRight, RedirectNumberMapIp2Tel_LeaveFromRight, RedirectNumberMapIp2Tel_Prefix2Add, RedirectNumberMapIp2Tel_Suffix2Add, RedirectNumberMapIp2Tel_IsPresentationRestricted; [RedirectNumberMapIp2Tel] For example: RedirectNumberMapIp2Tel 1 = *, 88, *, 1, 1, 2, 0, 255, 9, , 255; Notes:

Parameter	Description
	<ul style="list-style-type: none"> ▪ This parameter table can include up to 20 indices (1-20). ▪ If the table's characteristics rule (i.e., DestinationPrefix, RedirectPrefix, and SourceAddress) matches the IP-to-Tel call, then the redirect number manipulation rule (defined by the other parameters) is applied to the call. ▪ The manipulation rules are done in the following order: RemoveFromLeft, RemoveFromRight, LeaveFromRight, Prefix2Add, and then Suffix2Add. ▪ The RedirectPrefix parameter is used before any manipulation has been performed on it.
Redirect Number Tel-to-IP Table	
Web: Redirect Number Tel -> IP EMS: Redirect Number Map Tel to IP [RedirectNumberMapTel2IP]	<p>This parameter table 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:</p> <pre>[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]</pre> <p>For example: RedirectNumberMapTel2Ip 1 = *, 4, 255, 255, 0, 0, 255, , 972, 255, 1, 2;</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 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 parameters NumberType and NumberPlan are applicable only to the SIP Resource-Priority header.
Phone Context Table	
Web: Phone Context Table EMS: SIP Manipulations > Phone	This <i>parameter</i> table defines the Phone Context table. This parameter maps NPI and TON to the SIP Phone-Context

Parameter	Description
Context [PhoneContext]	<p>parameter. When a call is received from the ISDN/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.</p> <p>The format for this parameter is as follows: [PhoneContext] FORMAT PhoneContext_Index = PhoneContext_Npi, PhoneContext_Ton, PhoneContext_Context; [PhoneContext]</p> <p>For example: PhoneContext 0 = 0,0,unknown.com PhoneContext 1 = 1,1,host.com PhoneContext 2 = 9,1,na.e164.host.com</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 262. ▪ For a description on using <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.
Web/EMS: Add Phone Context As Prefix [AddPhoneContextAsPrefix]	<p>Determines whether the received Phone-Context parameter is added as a prefix to the outgoing ISDN Setup message with (for digital interfaces) Called and Calling numbers.</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default). ▪ [1] Enable = Enable.

A.12.16 LDAP Parameters

The Lightweight Directory Access Protocol (LDAP) parameters are described in the table below. For more information on routing based on LDAP, refer to 'Routing Based on LDAP Active Directory Queries' on page 177.

Table A-70: LDAP Parameters

Parameter	Description
Web: LDAP Service [LDAPServiceEnable]	<p>Enables the LDAP feature.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: LDAP Server IP [LDAPServerIP]	<p>Defines the LDAP server's IP address in dotted-decimal notation (e.g., 192.10.1.255). The default is 0.0.0.0.</p>

Parameter	Description
Web: LDAP Server Port [LDAPServerPort]	Defines the LDAP server's port number. The valid value range is 0 to 65535. The default port number is 389.
Web: LDAP Server Domain Name [LDAPServerDomainName]	Defines the host name of the LDAP server.
Web: LDAP Password [LDAPPassword]	Defines the LDAP server's user password.
Web: LDAP Bind DN [LDAPBindDN]	Defines the LDAP server's bind DN. This is used as the username during connection and binding to the server. For example: LDAPBindDN = "CN=Search user,OU=Labs,DC=OCSR2,DC=local"
Web: LDAP Search Dn [LDAPSearchDN]	Defines the search DN for LDAP search requests. This is the top DN of the subtree where the search is performed. This parameter is mandatory for the search. For example: LDAPSearchHDN = "CN=Search user,OU=Labs,DC=OCSR2,DC=local"
Web: LDAP Server Max Respond Time [LDAPServerMaxRespondTime]	Defines the time (in seconds) that the device waits for LDAP server responses. The valid value range is 0 to 86400. The default is 3000.
[LDAPDebugMode]	Determines whether to enable the LDAP task debug messages. This is used for providing debug information regarding LDAP tasks. The valid value range is 0 to 3. The default is 0.
Web: MS LDAP OCS Number attribute name [MSLDAPOCSNumAttributeName]	Defines the name of the attribute that represents the user OCS number in the Microsoft AD database. The valid value is a string of up to 49 characters. The default is "msRTC SIP-PrimaryUserAddress".
Web: MS LDAP PBX Number attribute name [MSLDAPPBXNumAttributeName]	Defines the name of the attribute that represents the user PBX number in the Microsoft AD database. The valid value is a string of up to 49 characters. The default is "telephoneNumber".
Web: MS LDAP MOBILE Number attribute name [MSLDAPMobileNumAttributeName]	Defines the name of the attribute that represents the user Mobile number in the Microsoft AD database. The valid value is a string of up to 49 characters. The default is "mobile".

A.12.17 Least Cost Routing Parameters

The Least Cost Routing parameters are described in the table below.

Table A-71: LCR Parameters

Parameter	Description
Web: Routing Rule Groups Table [RoutingRuleGroups]	This parameter table enables the LCR feature and configures the average call duration and default call cost. The default call cost determines whether routing rules that are not configured with a Cost Group are considered as a higher or lower cost route compared to other matching routing rules that are assigned Cost Groups. [RoutingRuleGroups] FORMAT RoutingRuleGroups_Index = RoutingRuleGroups_LCREnable, RoutingRuleGroups_LCRAverageCallLength, RoutingRuleGroups_LCRDefaultCost; [\RoutingRuleGroups]
Web: Cost Group Table [CostGroupTable]	This parameter table configures the Cost Groups for LCR, where each Cost Group is configured with a name, fixed call connection charge, and a call rate (charge per minute). [CostGroupTable] FORMAT CostGroupTable_Index = CostGroupTable_CostGroupName, CostGroupTable_DefaultConnectionCost, CostGroupTable_DefaultMinuteCost; [\CostGroupTable] For example: CostGroupTable 2 = "Local Calls", 2, 1;
Web: Cost Group > Time Band Table [CostGroupTimebands]	This parameter table configures time bands and associates them with Cost Groups [CostGroupTimebands] FORMAT CostGroupTimebands_TimebandIndex = CostGroupTimebands_StartTime, CostGroupTimebands_EndTime, CostGroupTimebands_ConnectionCost, CostGroupTimebands_MinuteCost; [\CostGroupTimebands]

A.13 Standalone Survivability Parameters

The Stand-alone Survivability (SAS) parameters are described in the table below.

Table A-72: SAS Parameters

Parameter	Description
Web: Enable SAS EMS: Enable [EnableSAS]	Enables the Stand-Alone Survivability (SAS) feature. <ul style="list-style-type: none"> ▪ [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.

Parameter	Description
	Note: For this parameter to take effect, a device reset is required.
Web: SAS Local SIP UDP Port EMS: Local SIP UDP [SASLocalSIPUDPPort]	Defines the local UDP port for sending and receiving SIP messages for SAS. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port. The valid range is 1 to 65,534. The default value is 5080.
Web: SAS Default Gateway IP EMS: Default Gateway IP [SASDefaultGatewayIP]	Defines the Default Gateway used in SAS 'Emergency Mode'. When an incoming SIP INVITE is received and the destination Address-Of-Record is not included in the SAS database, the request is immediately sent to this default gateway. The address can be configured as an IP address (dotted-decimal notation) or as a domain name (up to 49 characters). You can also configure the IP address with a destination port, e.g., "10.1.2.3:5060". The default is a null string, i.e., the local IP address of the gateway.
Web: SAS Registration Time EMS: Registration Time [SASRegistrationTime]	Defines the value of the SIP Expires header that is sent in a 200 OK response to an incoming REGISTER message when in SAS 'Emergency Mode'. The valid range is 0 (Analog) or 10 (Digital) to 2,000,000. The default value is 20.
Web: SAS Local SIP TCP Port EMS: Local SIP TCP Port [SASLocalSIPTCPPort]	Defines the local TCP port used to send/receive SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port. 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]	Defines the local TLS port used to send/receive SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port. 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. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>The Record-Route header is inserted in a request by a SAS proxy to force future requests in the dialog session to be routed through the SAS agent. Each traversed proxy in the path can insert this header, causing all future dialogs in the session to pass through it as well.</p> <p>When this feature is enabled, the SIP Record-Route header includes the URI "lr" parameter, indicating loose routing, for example:</p> <pre>Record-Route: <sip:server10.biloxi.com;lr></pre>
Web: SAS Proxy Set EMS: Proxy Set	Defines the Proxy Set (index number) used in SAS Normal mode to forward REGISTER and INVITE requests from users

Parameter	Description
[SASProxySet]	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]	Defines the Proxy Set (index number) used in SAS Emergency mode for fallback when the user is not found in the Registered Users database. Each time a new SIP request arrives, the SAS application checks whether the user is listed in the registration database. If the user is located in the database, the request is sent to the user. If the user is not found, the request is forwarded to the next redundant SAS defined in the Redundant SAS Proxy Set. If that SAS Proxy IP appears in the Via header of the request, it is not forwarded (thereby, preventing loops in the request's course). If no such redundant SAS exists, the SAS sends the request to its default gateway (configured by the parameter SASDefaultGatewayIP). 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. <ul style="list-style-type: none"> ▪ [0] Un-Block = Allow INVITE from unregistered SAS users (default). ▪ [1] Block = Reject dialog-establishment requests from unregistered 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. <ul style="list-style-type: none"> ▪ [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. <p>Note: Operating in this mode causes all incoming dialog requests to traverse the SAS, which may cause load problems.</p>
Web: SAS Survivability Mode EMS: Survivability Mode [SASSurvivabilityMode]	Determines the Survivability mode used by the SAS application. <ul style="list-style-type: none"> ▪ [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 (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.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [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]	<p>Enables SAS to perform ENUM (E.164 number to URI mapping) queries when receiving INVITE messages in SAS emergency mode.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Web: SAS Binding Mode EMS: Binding Mode [SASBindingMode]	<p>Determines the SAS application database binding mode.</p> <ul style="list-style-type: none"> ▪ [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]	<p>Defines emergency numbers for the device's SAS application. When the device's SAS agent receives a SIP INVITE (from an IP phone) that includes one of the emergency numbers (in the SIP user part), it forwards the INVITE to the default gateway (configured by the parameter SASDefaultGatewayIP), i.e., the device itself, which sends the call directly to the PSTN. This is important for routing emergency numbers such as 911 (in North America) directly to the PSTN. This is applicable to SAS operating in Normal and Emergency modes.</p> <p>Up to four emergency numbers can be defined, where each number can be up to four digits.</p>
[SASEmergencyPrefix]	<p>Defines a prefix that is added to the Request-URI user part of the INVITE message that is sent by the device's SAS agent when in Emergency mode to the default gateway or to any other destination (using the 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.</p> <p>This valid value is a character string. The default is an empty string "".</p>
Web: SAS Inbound Manipulation Mode [SASInboundManipulationMode]	<p>Enables destination number manipulation in incoming INVITE messages when SAS is in Emergency the state. The manipulation rule is done in the IP to IP Inbound Manipulation table.</p> <ul style="list-style-type: none"> ▪ [0] = None (default) ▪ [1] = Emergency only <p>Notes:</p> <ul style="list-style-type: none"> ▪ Inbound manipulation applies only to INVITE requests. ▪ For more information on SAS inbound manipulation, see 'Manipulating Destination Number of Incoming INVITE' on page 387.

Parameter	Description
SAS Registration Manipulation Table	
Web: SAS Registration Manipulation EMS: Stand-Alone Survivability [SASRegistrationManipulation]	<p>This <i>parameter</i> table 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:</p> <pre>[SASRegistrationManipulation] FORMAT SASRegistrationManipulation_Index = SASRegistrationManipulation_RemoveFromRight, SASRegistrationManipulation_LeaveFromRight; [\\SASRegistrationManipulation]</pre> <ul style="list-style-type: none"> ▪ 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. <p>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.</p> <p>For example, the manipulation rule below routes an INVITE with Request-URI header "sip:7184002@10.33.4.226" to user "4002@10.33.4.226" (i.e., keep only four digits from right of user part):</p> <pre>SASRegistrationManipulation 0 = 0, 4;</pre> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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 'Manipulating Destination Number of Incoming INVITE' on page 387.
Web: SAS IP-to-IP Routing Table	
[IP2IPRouting]	<p>This <i>parameter</i> table configures the IP-to-IP Routing table for SAS routing rules. The format of this parameter is as follows:</p> <pre>[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]</pre> <p>For example:</p> <pre>IP2IPRouting 1 = -1, *, *, *, *, 0, -1, -1, , 0, -1, 0;</pre> <p>Notes:</p> <ul style="list-style-type: none"> ▪ 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,

Parameter	Description
	<p>see 'Configuring IP2IP Routing Table (SAS)' on page 389.</p> <ul style="list-style-type: none"> For a description on configuring <i>ini</i> file table parameters, see 'Configuring ini File Table Parameters' on page 84.

A.14 IP Media Parameters

The IP media parameters are described in the table below.

Table A-73: IP Media Parameters

Parameter	Description
Web: Number of Media Channels EMS: Media Channels [MediaChannels]	<p>Defines the number of DSP channels that are allocated for various functionality (IP streaming, IP conferencing, IP transcoding, IP-to-IP sessions).</p> <p>The RTP streams for IP-to-IP calls always transverse through the device and two DSP channels are allocated per IP-to-IP session. Therefore, the maximum number of media channels for IP-to-IP calls is 120, corresponding to 60 IP-to-IP calls.</p> <p>The maximum value for media channels depends on the number of installed Media Processing modules (MPM): 1 module = 20 channels; 2 modules = 60; 3 modules = 100.</p> <p>The default value is 0.</p> <p>Notes:</p> <ul style="list-style-type: none"> For this parameter to take effect, a device reset is required. Other DSP channels can be used for PSTN interfaces. For a description on DSP utilization for IP-to-IP calls, see DSP Channel DSP Channel Resources for IP-to-IP Routing.
[EnableIPMediaChannels]	<p>Enables IP media channel support.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable only to Mediant 1000. For this parameter to take effect, a device reset is required.
[IPmediaChannels]	<p>This ini file parameter table defines the number of DSP channels that are "borrowed" from each of the device's digital modules for IP media functionality. The format of this parameter is as follows:</p> <pre>[IPMediaChannels] FORMAT IPMediaChannels_Index = IPMediaChannels_ModuleID, IPMediaChannels_DSPChannelsReserved; [\IPMediaChannels]</pre> <p>For example, the below settings use 15 and 10 DSP channels from modules 1 and 2, respectively:</p> <pre>IPMediaChannels 1 = 1, 15; IPMediaChannels 2 = 2, 10;</pre> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable only to Mediant 1000. The value of DSPChannelsReserved must be in multiples of 5 (since the reservation is done per DSP device and not per DSP channel).

Parameter	Description
	<ul style="list-style-type: none"> ▪ By default, the MPM module is set to the maximum value of IPM channels, therefore, there is no need to define it. ▪ By default, a digital module (i.e., TRUNKS module) is set to 0 IPM channels. ▪ For DSP utilization options, see DSP Channel DSP Channel Resources for IP-to-IP Routing.
Web: Enable Voice Streaming [EnableVoiceStreaming]	Enables the HTTP Voice Streaming application (play/record). <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable. Note: For this parameter to take effect, a device reset is required.
[VoiceStreamUploadMethod]	Defines the HTTP request type for loading the voice stream to the file server. <ul style="list-style-type: none"> ▪ [0] = POST (default). ▪ [1] = PUT. Notes: <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is applicable only to MSCML recording.
[VoiceStreamUploadPostURI]	Defines the URI used on the POST request to upload voice data from the media server to a Web server. Note: For this parameter to take effect, a device reset is required.
[APSEnabled]	Determines whether Voice Prompt index references refer to audio provided by the Audio Provisioning Server (APS) or by the local Voice Prompts file. <ul style="list-style-type: none"> ▪ [0] = APS disabled. Local Voice Prompts file is used. An audio reference in a play request (such as http://localhost/0) indicates that the Voice Prompt at index 0 in the Voice Prompts file is played. ▪ [1] = APS enabled (default). An audio reference (such as http://localhost/99) indicates that the audio segment provisioned on the APS with segment ID 99 is played. Note: For this parameter to take effect, a device reset is required.
Web: Calling Number Playback ID [CallingNumberPlayBackID]	Defines the Calling Number identification string for local, audio playing of the calling number. When the device receives from the Application Server (or SIP user Agent) a regular SIP INVITE message with a SIP URI that includes this user-defined Calling Number identification string, the device plays the calling number to the phone. <p>For example, upon the receipt of the below INVITE message, the device plays the numbers 1, 0, and then 1:</p> <pre>INVITE sip:callingnumber@domain.com; From: <sip:101@10.132.11.245>;</pre> <p>The valid value can be up to 16 characters. The default is "callingnumber".</p> <p>Note: The APS server support must be enabled to support this feature. Below are the relevant ini file parameter settings:</p> <ul style="list-style-type: none"> ▪ CallingNumberPlayBackID = callingnumber ▪ VpFileUrl = 'http://10.132.10.46/vp.dat' ▪ APSSegmentsFileURL = 'http://10.132.10.46/segments.xml' ▪ APSEnabled = 1

Parameter	Description
	<ul style="list-style-type: none"> ▪ AMSProfile = 1 ▪ AASPackagesProfile = 3 ▪ EnableVoiceStreaming = 1
Web: NetAnn Announcement ID [NetAnnAnncID]	<p>Defines the NetAnn identification string (up to 16 characters) for playing an announcement using the NetAnn interface. The application server sends a regular SIP INVITE message with a SIP URI that includes this identifier string and a "play=" parameter that identifies the necessary announcement. The default value is 'annc'.</p> <p>Example 1: INVITE sip: annc@10.2.3.4;play=http://localhost/1. Example 2: INVITE sip: annc@10.2.3.4;play=http://10.2.3.4/Annc/hello.wav.</p>
Web: MSCML ID [MSCMLID]	<p>Defines the Media Server Control Markup Language (MSCML) identification string (up to 16 characters). To start an MSCML session, the application server sends a regular SIP INVITE message with a SIP URI that includes this string. The default value is 'ivr'.</p> <p>For example: INVITE sip:ivr@10.2.3.4 Subsequent INFO messages carry the requests and responses.</p>
Web: Transcoding ID [TranscodingID]	<p>Defines the Transcoding identification string (up to 16 characters) used for identifying an incoming Transcoding call. The default value is 'trans'.</p> <p>For more information on Transcoding, see NetAnn Interface on page 414.</p>
AMS Parameters	
[AmsProfile]	<p>Enables advanced audio.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable <p>Note: For this parameter to take effect, a device reset is required.</p>
[AASPackagesProfile]	<p>Must be set to 3 to use advanced audio.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[AmsPrimaryLanguage]	<p>Determines the primary language used in the advanced audio package. The default value is "eng". The languages are according to ISO standard 639-2 language codes.</p>
[AmsSecondaryLanguage]	<p>Determines the secondary language used in the advanced audio package. The default value is "heb". The languages are according to ISO standard 639-2 language codes.</p>
[AMSAllowUriAsAlias]	<p>Determines whether or not play requests for remote URLs are first verified with local audio segments to determine if any have an alias matching for the URL. If a match is found, the corresponding local audio segment is played.</p> <ul style="list-style-type: none"> ▪ [0] = Always use remote storage (default). ▪ [1] = Check local storage first. <p>One application for this capability is that of a 'provisioned' cache within the device. For details on provisioning an alias and other audio</p>

Parameter	Description
	provisioning capabilities, refer to the Audio Provisioning Server (APS) User's Manual.
Conferencing Parameters	
Web/EMS: Conference ID [ConferenceID]	<p>Defines the Conference Identification string (up to 16 characters). The default value is 'conf'.</p> <p>For example: ConferenceID = MyConference</p> <p>Note: To join a conference, the INVITE URI must include the Conference ID string, preceded by the number of the participants in the conference, and terminated by a unique number.</p> <p>For example: Invite sip:4MyConference1234@10.1.10.10.</p> <p>INVITE messages with the same URI join the same conference.</p>
Web: Beep on Conference [BipOnConference]	<p>Determines whether or not a beep is played when a participant joins or leaves a conference (in the latter case, a beep of a different pitch is heard).</p> <ul style="list-style-type: none"> ▪ [0] Disable = Beep is disabled. ▪ [1] Enable = Beep is enabled (default).
Web: Enable Conference DTMF Clamping [EnableConferenceDTMFClamp]	<p>Determines the device logic once a DTMF is received on any conference participant. If enabled, the DTMF is not regenerated toward the other conference participants. This logic is only relevant for simple conferencing (NetAnn).</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable ▪ [1] Enable = Enable (default)
Web: Enable Conference DTMF Reporting [EnableConferenceDTMFReporting]	<p>Determines the device logic once a DTMF is received on any conference participant. If enabled, the device reports this DTMF in an out-of-band SIP message (according to TxDTMFOptions). This logic is only relevant for simple conferencing (NetAnn).</p> <ul style="list-style-type: none"> ▪ [0] Disable = Disable (default) ▪ [1] Enable = Enable
Web: Active Speakers Min. Interval [ActiveSpeakersNotificationMinInterval]	<p>Defines the minimum interval (in 100 msec units) between each Active Speaker Notification (ASN) events report. These events report on the active speakers in a conference. The event is issued whenever the active speakers change.</p> <p>Minimum configurable interval between events is 500 msec (5 units). The range is 5 to 2147483647 units. The default is 20 (i.e., 100 msec).</p>
Web: Playback Audio Format [cpPlayCoder]	<p>Determines the coder when playing a RAW file.</p> <ul style="list-style-type: none"> ▪ [1] G711 Mulaw ▪ [2] G711 Alaw (default)
Web: Record Audio Format [cpRecordCoder]	<p>Determines the coder for recording all supported file types.</p> <ul style="list-style-type: none"> ▪ [1] G711 Mulaw ▪ [2] G711 Alaw (default) <p>Note: For this parameter to take effect, a device reset is required.</p>
Web: End of Record Trim [cpEndOfRecordCutTime]	<p>Defines the maximum amount (in milliseconds) of audio to remove from the end of a recording. This is used to remove the DTMF signals generated by the end user for terminating the record. The valid range is 0 to 65,535. The default is 0.</p>
[NFSCClientMaxRetransmission]	<p>Since NFS is carried over UDP, retransmission is performed for messages without a response. This parameter enables the user to define the maximum number of retransmissions performed for such a</p>

Parameter	Description
	command. By default, the parameter is not used and the number of retransmissions is derived from the parameter <code>ServerRespondTimeout</code> . The range is 1 to 100. The default is 0 (derived from <code>ServerRespondTimeout</code>).
[StreamingPlayingUnderRunTimeout]	Defines the maximum time (in msec) that the device waits for the streaming server to acknowledge data sent to it. The range is 100 to 10,000. The default is 5,000.
[StreamingRecordingOverRunTimeout]	Defines the maximum time (in msec) that the streaming server waits to acknowledge a data request sent from the device. The range is 100 to 10,000. The default is 5,000.
[ServerRespondTimeout]	Defines the maximum time (in msec) that the device must wait for a response when operating with a remote server. The valid range is 1,000 to 90,000. The default is 5,000.
Automatic Gain Control (AGC) Parameters	
Web: Enable AGC EMS: AGC Enable [EnableAGC]	<p>Enables the AGC mechanism. The AGC mechanism adjusts the level of the received signal to maintain a steady (configurable) volume level.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Enable. <p>Notes:</p> <ul style="list-style-type: none"> ▪ This parameter can also be configured per Tel Profile, using the <code>TelProfile</code> parameter. ▪ For a description of AGC, see Automatic Gain Control (AGC) on page 164.
Web: AGC Slope EMS: Gain Slope [AGCGainSlope]	<p>Determines the AGC convergence rate:</p> <ul style="list-style-type: none"> ▪ [0] 0 = 0.25 dB/sec ▪ [1] 1 = 0.50 dB/sec ▪ [2] 2 = 0.75 dB/sec ▪ [3] 3 = 1.00 dB/sec (default) ▪ [4] 4 = 1.25 dB/sec ▪ [5] 5 = 1.50 dB/sec ▪ [6] 6 = 1.75 dB/sec ▪ [7] 7 = 2.00 dB/sec ▪ [8] 8 = 2.50 dB/sec ▪ [9] 9 = 3.00 dB/sec ▪ [10] 10 = 3.50 dB/sec ▪ [11] 11 = 4.00 dB/sec ▪ [12] 12 = 4.50 dB/sec ▪ [13] 13 = 5.00 dB/sec ▪ [14] 14 = 5.50 dB/sec ▪ [15] 15 = 6.00 dB/sec ▪ [16] 16 = 7.00 dB/sec ▪ [17] 17 = 8.00 dB/sec ▪ [18] 18 = 9.00 dB/sec ▪ [19] 19 = 10.00 dB/sec ▪ [20] 20 = 11.00 dB/sec ▪ [21] 21 = 12.00 dB/sec

Parameter	Description
	<ul style="list-style-type: none"> ▪ [22] 22 = 13.00 dB/sec ▪ [23] 23 = 14.00 dB/sec ▪ [24] 24 = 15.00 dB/sec ▪ [25] 25 = 20.00 dB/sec ▪ [26] 26 = 25.00 dB/sec ▪ [27] 27 = 30.00 dB/sec ▪ [28] 28 = 35.00 dB/sec ▪ [29] 29 = 40.00 dB/sec ▪ [30] 30 = 50.00 dB/sec ▪ [31] 31 = 70.00 dB/sec
Web: AGC Redirection EMS: Redirection [AGCRedirection]	Determines the AGC direction. <ul style="list-style-type: none"> ▪ [0] 0 = AGC works on signals from the TDM side (default). ▪ [1] 1 = AGC works on signals from the IP side.
Web: AGC Target Energy EMS: Target Energy [AGCTargetEnergy]	Defines the signal energy value (dBm) that the AGC attempts to attain. The valid range is 0 to -63 dBm. The default value is -19 dBm.
EMS: Minimal Gain [AGCMinGain]	Defines the minimum gain (in dB) by the AGC when activated. The range is 0 to -31. The default is -20. Note: For this parameter to take effect, a device reset is required.
EMS: Maximal Gain [AGCMaxGain]	Defines the maximum gain (in dB) by the AGC when activated. The range is 0 to 18. The default is 15. Note: For this parameter to take effect, a device reset is required.
EMS: Disable Fast Adaptation [AGCDisableFastAdaptation]	Enables the AGC Fast Adaptation mode. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable Note: For this parameter to take effect, a device reset is required.
Answer Machine Detector (AMD) Parameters	
Web: Web: Answer Machine Detector Sensitivity Parameter Suite [AMDSensitivityParameterSuite]	Determines the AMD Parameter Suite that you want the device to use. <ul style="list-style-type: none"> ▪ [0] = USA Parameter Suite with 8 detection sensitivity levels (from 0 to 7). (default) ▪ [1] = USA Parameter Suite with high detection sensitivity resolution (16 sensitivity levels, from 0 to 15). ▪ [2]-[3] = Other countries parameter suites with up to 16 sensitivity levels. Notes: <ul style="list-style-type: none"> ▪ The sensitivity level is selected by the AMDSensitivityLevel parameter. ▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see Configuring IP Profiles on page 217).
Web: Answer Machine Detector Sensitivity Level [AMDSensitivityLevel]	Defines the AMD detection sensitivity level of the selected AMD Parameter Suite. The valid value range is 0 (for best detection of an answering machine) to 15 (for best detection of a live call). The default value is 8. Notes: <ul style="list-style-type: none"> ▪ This parameter is applicable only if the AMDSensitivityParameterSuite parameter is set to any option other

Parameter	Description
	<p>than 0.</p> <ul style="list-style-type: none"> This parameter can also be configured per IP Profile, using the IPProfile parameter (see Configuring IP Profiles on page 217).
<p>Web: Answer Machine Detector Sensitivity EMS: Sensitivity [AMDDetectionSensitivity]</p>	<p>Defines the AMD detection sensitivity level of the selected Parameter Suite.</p> <p>AMD can be useful in automatic dialing applications. In some of these applications, it is important to detect if a human voice or an answering machine is answering the call. AMD can be activated and de-activated only after a channel is already open.</p> <p>The valid value range is 0 to 7, where 0 is the best detection for answering machines and 7 is the best detection for live calls (i.e., voice detection). The default is 3.</p> <p>Notes:</p> <ul style="list-style-type: none"> This parameter is applicable only if the AMDSensitivityParameterSuit parameter is set to 0. To enable the AMD feature, set the EnabledDSPIPMDetectors parameter to 1. For more information on AMD, see Answer Machine Detector (AMD) on page 160.
<p>Web: AMD Sensitivity File [AMDSensitivityFileName]</p>	<p>Defines the name of the AMD Sensitivity file that contains the AMD Parameter Suites.</p> <p>Notes:</p> <ul style="list-style-type: none"> This file must be in binary format (.dat). You can use the DConvert utility to convert the original file format from XML to .dat. You can load this file using the Web interface (see Loading Auxiliary Files on page 471).
<p>[AMDSensitivityFileUrl]</p>	<p>Defines the URL path to the AMD Sensitivity file for downloading from a remote server.</p>
<p>[AMDMinimumVoiceLength]</p>	<p>Defines the AMD minimum voice activity detection duration (in 5-ms units). Voice activity duration below this threshold is ignored and considered as non-voice.</p> <p>The valid value range is 10 to 100. The default is 42 (i.e., 210 ms).</p>
<p>[AMDMaxGreetingTime]</p>	<p>Defines the maximum duration to detect greeting message.</p> <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see Configuring IP Profiles on page 217).</p>
<p>[AMDMaxPostGreetingSilenceTime]</p>	<p>Defines the maximum duration of silence from after the greeting time is over (defined by AMDMaxGreetingTime) until the AMD decision.</p> <p>Note: This parameter can also be configured per IP Profile, using the IPProfile parameter (see Configuring IP Profiles on page 217).</p>
<p>EMS: Time Out [AMDTimeout]</p>	<p>Defines the timeout (in msec) between receiving Connect messages from the ISDN and sending AMD results.</p> <p>The valid range is 1 to 30,000. The default is 2,000 (i.e., 2 seconds).</p>
<p>Web/EMS: AMD Beep Detection Mode [AMDBeepDetectionMode]</p>	<p>Determines the AMD beep detection mode. This mode detects the beeps played at the end of an answering machine message, by using the X-Detect header extension. The device sends a SIP INFO message containing the field values Type=AMD and SubType=Beep. This feature allows users of certain third-party, Application server to leave a voice message after an answering machine plays the "beep".</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ [0] Disabled (default) ▪ [1] Start After AMD ▪ [2] Start Immediately
Web: Answer Machine Detector Beep Detection Timeout EMS: Beep Detection Timeout [AMDBeepDetectionTimeout]	Defines the AMD beep detection timeout (i.e., the duration that the beep detector functions from when detection is initiated). This is used for detecting beeps at the end of an answering machine message. The valid value is in units of 100 milliseconds, from 0 to 1638. The default value is 200 (i.e., 20 seconds).
Web: Answer Machine Detector Beep Detection Sensitivity EMS: Beep Detection Sensitivity [AMDBeepDetectionSensitivity]	Defines the AMD beep detection sensitivity for detecting beeps at the end of an answering machine message. The valid value is 0 to 3, where 0 (default) is the least sensitive.
Energy Detector Parameters Note: Currently, this feature is not supported.	
Enable Energy Detector [EnableEnergyDetector]	Enables the Energy Detector feature. This feature generates events (notifications) when the signal received from the PSTN is higher or lower than a user-defined threshold (defined by the EnergyDetectorThreshold parameter). <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Energy Detector Quality Factor [EnergyDetectorQualityFactor]	Defines the Energy Detector's sensitivity level. The valid range is 0 to 10, where 0 is the lowest sensitivity and 10 the highest sensitivity. The default is 4.
Energy Detector Threshold [EnergyDetectorThreshold]	Defines the Energy Detector's threshold. A signal below or above this threshold invokes an 'Above' or 'Below' event. The threshold is calculated as follows: Actual Threshold = -44 dBm + (EnergyDetectorThreshold * 6) The valid value range is 0 to 7. The default is 3 (i.e., -26 dBm).
Pattern Detection Parameters Note: For an overview on the pattern detector feature for TDM tunneling, see DSP Pattern Detector on page 239.	
Web: Enable Pattern Detector [EnablePatternDetector]	Enables the Pattern Detector (PD) feature. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
[PDPattern]	Defines the patterns that can be detected by the Pattern Detector. The valid range is 0 to 0xFF. Note: For this parameter to take effect, a device reset is required.
[PDThreshold]	Defines the number of consecutive patterns to trigger the pattern detection event. The valid range is 0 to 31. The default is 5. Note: For this parameter to take effect, a device reset is required.

Parameter	Description
VXML Parameters	
Web/EMS: Enable VXML [EnableVXML]	Enables the VXML stack. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable Note: For this parameter to take effect, a device reset is required.
Web: VXML ID [VXMLID]	Defines the VoiceXML identification string (up to 16 characters) for identifying an incoming VXML call. The default value is 'dialog'.
[VxmlBargainAllowed]	Determines whether the VXML property indicates if prompts can be interrupted. <ul style="list-style-type: none"> [0] = prompts cannot be interrupted [1] = prompts can be interrupted (default) Note: For this parameter to take effect, a device reset is required.
[VxmlBuiltinGrammarPath]	Defines the path on the remote Automatic Speech Recognition (ASR) / text-to-speech (TTS) server to access the built-in grammars. The path must not end in a forward slash (/) as this is added as needed during runtime. The default value is NULL. Note: For this parameter to take effect, a device reset is required.
[VxmlCompleteTimeout]	Optional parameter that defines the amount of silence (in msec) to wait after speech grammar has been matched before reporting the match. The default value is 0 (i.e., don't set this parameter on recognition attempt). Note: For this parameter to take effect, a device reset is required.
[VxmlConfidenceLevel]	Defines the default speech recognition confidence threshold for VXML. The range is from 0 to 100. The default value is 50. Note: For this parameter to take effect, a device reset is required.
[VxmlDefaultLanguage]	Defines the default language for speech recognition, if speech recognition has been enabled. If the root document doesn't specify a language and a field or menu element generates speech recognition requests using the GRXML MIME type, the default language is used in the request. The default value is 'en_us'. Note: For this parameter to take effect, a device reset is required.
[VxmlIncompleteTimeout]	Optional parameter that defines the amount of silence (in msec) to wait after speech grammar has not matched a voice grammar. The default value is 0 (i.e., don't set this parameter on recognition attempt). Note: For this parameter to take effect, a device reset is required.
[VxmlInterDigitTimeout]	Defines the inter-digit timeout value (in msec) used when DTMF is received. The valid range for this parameter is 0 to 7,000 msec. The default value is 3,000. Note: For this parameter to take effect, a device reset is required.
[VxmlMaxActiveFiles]	Defines the maximum number of static VXML scripts that can be loaded to the system at any one time. The valid range for this parameter is 0 to 30. The default value is 10.

Parameter	Description
	<p>Note: This parameter does not affect the number of dynamic scripts that can be simultaneously active.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[VxmlMaxPorts]	<p>Defines the number of channels in the system that can simultaneously run VXML scripts. The range is from 0 to the maximum number of channels in the system. This value can be used to ensure there are sufficient VXML resources for each call. For example, if the system is running dynamic scripts that each requires many resources, the VxmlMaxPorts value can be lowered to help ensure that each individual call has adequate resources. The default value is 0.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[VxmlMaxSpeechTimeout]	<p>Defines the maximum time the caller can speak (in msec) in an attempt to match a speech grammar before a no match event is thrown. The range is 0 - 7,000. The default value is 0 (i.e., no time limit in the speech recognition attempt).</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[VxmlNoInputTimeout]	<p>Defines the no input timeout for digit (DTMF) collection or speech recognition (in msec). The range is 0 - 7,000. The default value is 3,000.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[VxmlSensitivityLevel]	<p>Defines the default speech recognition sensitivity level for VXML. The valid range for this parameter is 0 to 100. The default value is 50.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[VxmlSpeedVsAccuracy]	<p>Defines the hint to the speech recognition engine for the balance of speed vs. accuracy. The valid range is from 0 to 100. The default value is 50. A low number means the speech recognition engine must perform recognition rapidly, at the cost (i.e., trade off) of accuracy. A high number, such as 100, means the speech recognition engine must perform the speech recognition accurately, at the cost of speed.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[VxmlSystemInputModes]	<p>Determines which inputs are valid for grammars.</p> <ul style="list-style-type: none"> ▪ [0] = DTMF is valid (default) ▪ [1] = Voice is valid ▪ [2] = Both are valid <p>Note: For this parameter to take effect, a device reset is required.</p>
[VxmlTermChar]	<p>Defines the default terminating digit for received DTMF. The default value is 35 (equivalent to ASCII '#').</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[VxmlTermTimeout]	<p>Defines the time to wait before terminating received DTMF (in msec). The range is 0 - 7,000. The default value is 3,000.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>

Parameter	Description
Media Resource Control Protocol (MRCP) / Real Time Streaming Protocol (RTSP) Parameters	
[MRCPDefaultMIMETYPE]	Determines the default format for speech recognition for inline grammars. <ul style="list-style-type: none"> ▪ [0] = indicates GRXML (default) ▪ [1] = indicates GL (Nuance format)
[MRCPEnabled]	Activates the Media Resource Control Protocol (MRCP) functionality. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Activate
[MRCPMaxPorts]	Defines the number of ports that are allocated to running MRCP-related activities such as speech recognition and text-to-speech. A port is considered duplex, so that speech recognition and text-to-speech can run on the same port. The value should not exceed the number of channels in the system. The range is 0 - 120. The default value is 10.
[MRCPServerName]	Defines the hostname of the MRCP server. This is used to build a URI for the server. The default value is NULL.
[MRCPServerIp]	Defines the IP address of the MRCP speech server. The default value is 0.0.0.0.
[MRCPServerPort]	Defines the control port on the MRCP speech server. The range is 0 - 65,535. The default value is 554.
[RTSPConnectionRetryInterval]	Defines the time (in seconds) that the system must wait before trying to create a socket for the RTSP speech server if the socket was never created or was created and then brought down. The range is 0 - 65,535. The default value is 10. Note: For this parameter to take effect, a device reset is required.
[RTSPEnabled]	Activates the RTSP functionality. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Activate Note: For this parameter to take effect, a device reset is required.
[RTSPMaxPorts]	Defines the number of channels that can be simultaneously active in RTSP sessions. The range is 0 - 20. The default value is 10. Note: For this parameter to take effect, a device reset is required.

A.15 Auxiliary and Configuration Files Parameters

This subsection describes the device's auxiliary and configuration files parameters.

A.15.1 Auxiliary and 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. For loading these files using the *ini* file, you need to configure these files in the *ini* file and configured whether they must be stored in the non-volatile memory. The table below lists the *ini* file parameters associated with these auxiliary files. For more information on the auxiliary files, see 'Loading Auxiliary Files' on page 471.

Table A-74: Auxiliary and Configuration File Parameters

Parameter	Description
General Parameters	
[SetDefaultOnIniFileProcess]	<p>Determines if all the device's parameters are set to their defaults before processing the updated <i>ini</i> file.</p> <ul style="list-style-type: none"> ▪ [0] Disable - parameters not included in the downloaded <i>ini</i> file are not returned to default settings (i.e., retain their current settings). ▪ [1] Enable (default) <p>Note: This parameter is applicable only for automatic HTTP update or Web <i>ini</i> file upload (not applicable if the <i>ini</i> file is loaded using BootP).</p>
[SaveConfiguration]	<p>Determines if the device's configuration (parameters and files) is saved to flash (non-volatile memory).</p> <ul style="list-style-type: none"> ▪ [0] = Configuration isn't saved to flash memory. ▪ [1] = Configuration is saved to flash memory (default).
Auxiliary and Configuration File Name Parameters	
Web/EMS: Call Progress Tones File [CallProgressTonesFilename]	<p>Defines the name of the file containing the Call Progress Tones definitions. For more information on how to create and load this file, refer to the <i>Product Reference Manual</i>.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
Web/EMS: Voice Prompts File [VoicePromptsFileName]	<p>Defines the name (and path) of the file containing the Voice Prompts.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ This parameter is applicable only to Mediant 1000. ▪ For more information on this file, see Voice Prompts File on page 479.
Web/EMS: Prerecorded Tones File [PrerecordedTonesFileName]	<p>Defines the name (and path) of the file containing the Prerecorded Tones.</p> <p>Note: For this parameter to take effect, a device reset is required.</p>

Parameter	Description
Web: CAS File EMS: Trunk Cas Table Index [CASFileName_x]	Defines the CAS file name (e.g., 'E_M_WinkTable.dat'), which defines the CAS protocol (where x denotes the CAS file ID 0 to 7). It is possible to define up to eight different CAS files by repeating this parameter. Each CAS file can be associated with one or more of the device's trunks, using the parameter CASTableIndex or it can be associated per B-channel using the parameter CASChannelIndex. Note: For this parameter to take effect, a device reset is required.
Web: Dial Plan EMS: Dial Plan Name [CasTrunkDialPlanName_x]	Defines the Dial Plan name (up to 11-character strings) that is used on a specific trunk (denoted by x).
Web: Dial Plan File EMS: Dial Plan File Name [DialPlanFileName]	Defines the name (and path) of the Dial Plan file (defining dial plans). This file should be constructed using the DConvert utility (refer to the Product Reference Manual).
[UserInfoFileName]	Defines the name (and path) of the file containing the User Information data.

A.15.2 Automatic Update Parameters

The automatic update of software and configuration files parameters are described in the table below.

Table A-75: Automatic Update of Software and Configuration Files Parameters

Parameter	Description
General Automatic Update Parameters	
[AutoUpdateCmpFile]	<p>Enables the Automatic Update mechanism for the cmp file.</p> <ul style="list-style-type: none"> [0] = The Automatic Update mechanism doesn't apply to the cmp file (default). [1] = The Automatic Update mechanism includes the cmp file. <p>Note: For this parameter to take effect, a device reset is required.</p>
[AutoUpdateFrequency]	<p>Defines the number of minutes that the device waits between automatic updates. The default value is 0 (i.e., the update at fixed intervals mechanism is disabled).</p> <p>Note: For this parameter to take effect, a device reset is required.</p>
[AutoUpdatePredefinedTime]	<p>Defines schedules (time of day) for automatic updates. The format of this parameter is: 'HH:MM', where <i>HH</i> depicts the hour and <i>MM</i> the minutes, for example, 20:18.</p> <p>Notes:</p> <ul style="list-style-type: none"> 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]	<p>Determines whether the Automatic Update mechanism verifies server certificates when using HTTPS.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable
[AUPDCheckIfIniChanged]	<p>Determines whether the Automatic Update mechanism performs CRC checking to determine if the <i>ini</i> file has changed prior to processing.</p> <ul style="list-style-type: none"> [0] = Do not check CRC. The <i>ini</i> file is loaded whenever the server provides it. (default) [1] = Check CRC for the entire file. Any change, including line order, causes the <i>ini</i> 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 <i>ini</i> file.
[ResetNow]	<p>Invokes an immediate device reset. This option can be used to activate offline (i.e., not on-the-fly) parameters that are loaded using the parameter <i>IniFileUrl</i>.</p> <ul style="list-style-type: none"> [0] = The immediate restart mechanism is disabled (default). [1] = The device immediately resets after an <i>ini</i> file with this parameter set to 1 is loaded.

Parameter	Description
Software/Configuration File URL Path for Automatic Update Parameters	
[CmpFileURL]	<p>Defines the name of the <i>cmp</i> file and the path to the server (IP address or FQDN) from where the device can load the <i>cmp</i> file and update itself. The <i>cmp</i> file can be loaded using HTTP/HTTPS, FTP, FTPS, or NFS.</p> <p>For example: <code>http://192.168.0.1/filename</code></p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ When this parameter is configured, the device always loads the <i>cmp</i> file after it is reset. ▪ The <i>cmp</i> file is validated before it's burned to flash. The checksum of the <i>cmp</i> file is also compared to the previously burnt checksum to avoid unnecessary resets. ▪ The maximum length of the URL address is 255 characters.
[IniFileURL]	<p>Defines the name of the <i>ini</i> file and the path to the server (IP address or FQDN) on which it is located. The <i>ini</i> file can be loaded using HTTP/HTTPS, FTP, FTPS, or NFS.</p> <p>For example: <code>http://192.168.0.1/filename</code> <code>http://192.8.77.13/config<MAC></code> <code>https://<username>:<password>@<IP address>/<file name></code></p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ For this parameter to take effect, a device reset is required. ▪ When using HTTP or HTTPS, the date and time of the <i>ini</i> file are validated. Only more recently dated <i>ini</i> files are loaded. ▪ The optional string <code><MAC></code> is replaced with the device's MAC address. Therefore, the device requests an <i>ini</i> file name that contains its MAC address. This option allows the loading of specific configurations for specific devices. ▪ The maximum length of the URL address is 99 characters.
[PrtFileURL]	<p>Defines the name of the Prerecorded Tones (PRT) file and the path to the server (IP address or FQDN) on which it is located.</p> <p>For example: <code>http://server_name/file</code>, <code>https://server_name/file</code>.</p> <p>Note: The maximum length of the URL address is 99 characters.</p>
[CptFileURL]	<p>Defines the name of the CPT file and the path to the server (IP address or FQDN) on which it is located.</p> <p>For example: <code>http://server_name/file</code>, <code>https://server_name/file</code>.</p> <p>Note: The maximum length of the URL address is 99 characters.</p>
[VpFileURL]	<p>Defines the name of the Voice Prompts file and the path to the server (IP address or FQDN) on which it is located.</p> <p>For example: <code>http://server_name/file</code>, <code>https://server_name/file</code>.</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ The maximum length of the URL address is 99 characters. ▪ This parameter is applicable only to Mediant 1000.
[CasFileURL]	<p>Defines the name of the CAS file and the path to the server (IP address or FQDN) on which it is located.</p> <p>For example: <code>http://server_name/file</code>, <code>https://server_name/file</code>.</p> <p>Note: The maximum length of the URL address is 99 characters.</p>

Parameter	Description
[TLSSRootFileUrl]	Defines the name of the TLS trusted root certificate file and the URL from where it can be downloaded. Note: For this parameter to take effect, a device reset is required.
[TLSCertFileUrl]	Defines the name of the TLS certificate file and the URL from where it can be downloaded. Note: For this parameter to take effect, a device reset is required.
[TLSPkeyFileUrl]	Defines the URL for downloading a TLS private key file using the Automatic Update facility.
[UserInfoFileURL]	Defines the name of the User Information file and the path to the server (IP address or FQDN) on which it is located. For example: http://server_name/file, https://server_name/file Note: The maximum length of the URL address is 99 characters.

B Dialing Plan Notation for Routing and Manipulation

The device supports flexible dialing plan notations for depicting the prefix and/or suffix source and/or destination numbers and SIP URI user names in the routing and manipulation tables.

Table B-1: Dialing Plan Notations for Prefixes and Suffixes

Notation	Description
x (letter "x")	Depicts any single digit.
# (pound symbol)	When used at the end of a prefix, it depicts the end of a number. For example, 54324xx# represents a 7-digit number that starts with the digits 54324. When used anywhere in the suffix, it is part of the number. For example, (3#45) can represent the number string, 123#45.
* (asterisk symbol)	When used in the prefix, it depicts any number. When used in the suffix, it is part of the number. For example, (3*45) can represent the number string, 123*45.
<p>Range of Digits</p> <p>Notes:</p> <ul style="list-style-type: none"> ▪ Dial plans depicting a prefix that is a range must be enclosed in square brackets, e.g., [4-8] or 23xx[456]. ▪ Dial plans depicting a prefix that is not a range is not enclosed, e.g., 12345#. ▪ Dial plans depicting a suffix must be enclosed in parenthesis, e.g., (4) and (4-8). ▪ Dial plans depicting a suffix that include multiple ranges, the range must be enclosed in square brackets, e.g., (23xx[4,5,6]). ▪ An example for entering a combined prefix and suffix dial plan - assume you want to match a rule whose destination phone prefix is 4 to 8, and suffix is 234, 235, or 236. The entered value would be the following: [4-8](23[4,5,6]). 	
[n-m] or (n-m)	<p>Represents a range of numbers. For example:</p> <ul style="list-style-type: none"> ▪ To depict numbers from 5551200 to 5551300: <ul style="list-style-type: none"> ✓ Prefix: [5551200-5551300]# ✓ Suffix: (5551200-5551300) ▪ To depict numbers from 123100 to 123200: <ul style="list-style-type: none"> ✓ Prefix: 123[100-200] ✓ Suffix: (123[100-200]) ▪ To depict prefix and suffix numbers together: <ul style="list-style-type: none"> ✓ 03(100): for any number that starts with 03 and ends with 100. ✓ [100-199](100,101,105): for a number that starts with 100 to 199 and ends with 100, 101 or 105. ✓ 03(abc): for any number that starts with 03 and ends with abc. ✓ 03(5xx): for any number that starts with 03 and ends with 5xx. ✓ 03(400,401,405): for any number that starts with 03 and ends with 400 or 401 or 405. <p>Notes:</p> <ul style="list-style-type: none"> ▪ The value <i>n</i> must be less than the value <i>m</i>. ▪ Only numerical ranges are supported (not alphabetical letters). ▪ For suffix ranges, the starting (<i>n</i>) and ending (<i>m</i>) numbers in the range

Notation	Description
	must have the same number of digits. For example, (23-34) is correct, but (3-12) is not.
[n,m,...] or (n,m,...)	Represents multiple numbers. For example, to depict a one-digit number starting with 2, 3, 4, 5, or 6: <ul style="list-style-type: none"> ▪ Prefix: [2,3,4,5,6]# ▪ Suffix: (2,3,4,5,6) ▪ Prefix with Suffix: [2,3,4,5,6](8,7,6) - prefix is denoted in square brackets; suffix in parenthesis For prefix only , the notations <i>d[n,m]e</i> and <i>d[n-m]e</i> can also be used: <ul style="list-style-type: none"> ▪ To depict a five-digit number that starts with 11, 22, or 33: [11,22,33]xxx# ▪ To depict a six-digit number that starts with 111 or 222: [111,222]xxx# Note: Up to three digits can be used to denote each number.
[n1-m1,n2-m2,a,b,c,n3-m3] or (n1-m1,n2-m2,a,b,c,n3-m3)	Represents a mixed notation of single numbers and multiple ranges. For example, to depict numbers 123 to 130, 455, 766, and 780 to 790: <ul style="list-style-type: none"> ▪ Prefix: [123-130,455,766,780-790] ▪ Suffix: (123-130,455,766,780-790) Note: The ranges and the single numbers used in the dial plan must have the same number of digits. For example, each number range and single number in the dialing plan example above consists of three digits.

C SIP Message Manipulation Syntax

This section provides a detailed description on the support and syntax for configuring SIP message manipulation rules. For configuring message manipulation rules, see the parameter MessageManipulations.

C.1 Actions

The actions that can be done on SIP message manipulation in the Message Manipulations table are listed in the table below.

Table C-1: Message Manipulation Actions

Action	Value
Add	0
Remove	1
Modify	2
Add Prefix	3
Add Suffix	4
Remove Suffix	5
Remove Prefix	6

The maximum length of the value for a manipulation is 299 characters.

C.2 Header Types

C.2.1 Accept

An example of the header is shown below:

```
Accept: application/sdp
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	No	N/A
Keyword	Sub Types		Attributes	
N/A	N/A		N/A	

Below is a header manipulation example:

Rule:	If the supported header does not contain 'mm,100rel,timer,replaces', then in all INVITE messages add an Accept header: <pre>MessageManipulations 8 = 1, invite, "header.supported != 'mm,100rel,timer,replaces'", header.accept, 0, ' application/x-private ', 0;</pre>
Result:	Accept: application/x-private

C.2.2 Accept-Language

An example of the header is shown below:

```
Accept-Language: da, en-gb;q=0.8, en;q=0.7
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	No	N/A
Keyword	Sub Types		Attributes	
N/A	N/A		N/A	

Below is a header manipulation example:

Rule:	Add a new Language header to all INVITE messages: <pre>MessageManipulations 0 = 1, invite, , header.accept-language, 0, "en, il, cz, it", 0;</pre>
Result:	Accept-Language: en, il, cz, it

C.2.3 Allow

An example of the header is shown below:

```
Allow:
REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUB
SCRIBE
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	No	N/A
Keyword	Sub Types		Attributes	
N/A	N/A		Read/Write	

Below is a header manipulation example:

Rule:	Add an Allow header to all INVITE messages: <pre>MessageManipulations 0 = 1, invite, , header.allow, 0, "REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INF O, SUBSCRIBE, XMESSAGE", 0;</pre>
Result:	Allow: REGISTER, OPTIONS, INVITE, ACK, CANCEL, BYE, NOTIFY, PRACK, REFER, INFO, SUBSCRIBE, XMESSAGE

C.2.4 Call-Id

An example of the header is shown below:

```
Call-ID: JN1YXOLCAIWTRHWOINNRR@10.132.10.128
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	No	No	No	NA

Keyword	Sub Types	Attributes
ID	String	Read Only

Below is a header manipulation example:

Rule:	Add a proprietary header to all INVITE messages using the data in the Call-id header: <pre>MessageManipulations 0 = 1, invite, , header.Xitsp-abc, 0, "header.call-id", 0;</pre>
Result:	Xitsp-abc: GIAPOFWRBQKJVAETIODI@10.132.10.128

C.2.5 Contact

An example of the header is shown below:

```
Contact: <sip:555@10.132.10.128:5080>
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	No	No	No	8

Keyword	Sub Types	Attributes
Expires	Integer	Read/Write
GruuContact	String	Read/Write
IsGRUU	Boolean	Read/Write
Name	String	Read/Write
Param	Param	Read/Write
URL	'URL' on page 795	Read/Write*

* Host name cannot be modified in the URL structure for a contact header.

Below is a header manipulation example:

Rule:	Change the user part in the Contact header in all INVITE messages to fred: <pre>MessageManipulations 0 = 1, Invite, ,header.contact.url.user, 2, "fred", 0;</pre>
Result:	Contact: <sip:fred@10.132.10.128:5070>

C.2.6 Cseq

An example of the header is shown below:

```
CSeq: 1 INVITE
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	No	No	No	N/A

Keyword	Sub Types	Attributes
Num	Integer	Read Only
Type	String	Read Only

Below is a header manipulation example:

Rule:	If the Cseq number is 1, then modify the user in the Contact header to fred. <pre>MessageManipulations 0 = 1, Invite, "header.cseq.num=='1",header.contact.url.user, 2, "'fred'", 0;</pre>
Result:	Contact: <sip:fred@10.132.10.128:5070>

C.2.7 Diversion

An example of the header is shown below:

```
Diversion: <sip:654@IPG2Host;user=phone>;reason=user-
busy;screen=no;privacy=off;counter=1
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	3

Keyword	Sub Types	Attributes
Name	String	Read/Write
Param	Param	Read/Write
Privacy	Enum Privacy (see 'Privacy' on page 800)	Read/Write
Reason	Enum Reason (see 'Reason (Diversion)' on page 800)	Read/Write
Screen	Enum Screen (see 'Screen' on page 803)	Read/Write
URL	URL Structure (see 'URL' on page 795)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Diversion header to all INVITE messages: <pre>MessageManipulations 0 = 1, invite, , header.Diversion, 0, " '<tel:+101>;reason=unknown; counter=1;screen=no; privacy=off'", 0;</pre>
	Result:	Diversion: <tel:+101>;reason=user- busy;screen=no;privacy=off;counter=1
Example 2	Rule:	Modify the Reason parameter in the header to 1, see 'Reason (Diversion)' on page 800 for possible values:

		MessageManipulations 1 = 1, invite, , header.Diversion.reason, 2, '1', 0;
	Result:	Diversion: <tel:+101>;reason=user-busy;screen=no;privacy=off;counter=1
Example 3	Rule:	The URL in the Diversion header is modified to that which is contained in the header URL: MessageManipulations 2 = 1, invite, , header.Diversion.URL, 2, "header.from.url", 0;
	Result:	Diversion:<sip:555@IPG2Host;user=phone>;reason=user-busy;screen=no;privacy=off;counter=1

C.2.8 Event

An example of the header is shown below:

```
Event: foo; id=1234
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
EventKey	Event Structure (see 'Event Structure' on page 793)	Read/Write
Param	Param	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add parameter itsp-abc=voip to the Event header: MessageManipulations 0 = 1, invite, , header.event.param.itsp-abc, 0, "'voip'" , 0;
	Result:	Event: foo;id=1234;itsp-abc=voip
Example 2	Rule:	Modify the Event ID string: MessageManipulations 1 = 1, invite, , header.event.EVENTKEY.id, 2, "'5678'", 0;
	Result:	Event: foo;id=5678;
Example 3	Rule:	Modify the Event package enum: MessageManipulations 2 = 1, invite, , header.event.EVENTKEY.EVENTPACKAGE, 2, "'2'", 0;
	Result:	Event: refer;id=5678

C.2.9 From

An example of the header is shown below:

```
From: <sip:555@10.132.10.128;user=phone>;tag=YQLQHCAAYBWKKRIVIMWEQ
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	No	No	No	NA

Keyword	Sub Types	Attributes
Name	String	Read/Write
Param	Param	Read/Write
tag	String	Read Only
URL	URL Structure (refer to 'URL' on page 795)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Change the user part of the From header if the user is not 654: <pre>MessageManipulations 8 = 1, invite, "header.from.url.user != '654'", header.from.url.user, 2, 'fred', 0;</pre>
	Result:	From: <sip:fred@IPG2Host;user=phone>;tag=1c20161
Example 2	Rule:	Add a new parameter to the From header called p1 and set its value to myParameter: <pre>MessageManipulations 1 = 1, Invite.request, ,header.from.param.p1, 0, "'myParameter'", 0;</pre>
	Result:	From: <sip:fred@IPG2Host;user=phone>;p1=myParameter;tag=1c5891
Example 3	Rule:	Modify the URL in the From header: <pre>MessageManipulations 0 = 1, any, , header.from.url, 2, 'sip:3200@110.18.5.41;tsunami=0', 0;</pre>
	Result:	From: <sip:3200@110.18.5.41;user=phone;tsunami=0>;tag=1c23750

C.2.10 History-Info

An example of the header is shown below:

```
History-Info: <sip:UserA@ims.example.com;index=1>
History-Info: <sip:UserA@audc.example.com;index=2>
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	20

Keyword	Sub Types	Attributes
HistoryInfo	String	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a new History-Info header to the message: <pre>MessageManipulations 0 = 1, any, , header.History-Info, 0, '<sip:UserA@audc.mydomain.com;index=3>', 0</pre>
	Result:	History-Info:sip:UserA@ims.example.com;index=1 History-Info:sip:UserA@audc.example.com;index=2 History-Info: <sip:UserA@audc.mydomain.com;index=3>
Example 2	Rule:	Delete an unwanted History-Info header from the message: <pre>MessageManipulations 0 = 1, any, , header.History-Info.1, 1, , 0;</pre>
	Result:	History-Info: <sip:UserA@ims.example.com;index=1>
Example 3	Rule:	Delete all History-Info from the message: <pre>MessageManipulations 0 = 1, any, , header.History-Info, 1, , 0;</pre>
	Result:	All history-info headers are removed.

C.2.11 Min-Se and Min-Expires

An example of the header is shown below:

```
Min-SE: 3600
Min-Expires: 60
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
Param	Param	Read/Write
Time	Integer	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Min-Se header to the message using a value of 50: <pre>MessageManipulations 1 = 1, any, , header.min-se, 0, '50', 0;</pre>
	Result:	Min-SE: 50
Example 2	Rule:	Modify a Min-Expires header with the min-expires value and add an additional 0: <pre>MessageManipulations 0 = 1, Invite, , header.Min-Expires.param, 2, "header.Min-Expires.time + '0'", 0;</pre>
	Result:	Min-Expires: 340;3400
Example 3	Rule:	Modify a Min-Expires header changing the time to 700: <pre>MessageManipulations 0 = 1, Invite, , header.Min-Expires.time, 2, "'700'", 0;</pre>
	Result:	Min-Expires: 700

C.2.12 P-Asserted-Identity

An example of the header is shown below:

```
P-Asserted-Identity: Jane Doe <sip:567@itasp.com>
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	1

Keyword	Sub Types	Attributes
URL	URL Structure (see 'URL' on page 795)	Read/Write
Name	String	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a P-Asserted-Id header to all INVITE messages: <pre>MessageManipulations 2 = 1, invite, , header.p-asserted-identity, 0, "'<sip:567@itasp.com>', 0;</pre>
	Result:	<pre>P-Asserted-Identity: <sip:567@itasp.com></pre>
Example 2	Rule:	Modify the P-Asserted-Identity host name to be the same as the host name in the To header: <pre>MessageManipulations 2 = 1, invite, , header.p-asserted-identity.URL.host, 2, header.to.url.host, 0;</pre>
	Result:	<pre>P-Asserted-Identity: <sip:567@10.132.10.128></pre>

C.2.13 P-Associated-Uri

An example of the header is shown below:

```
P-Associated-URI: <sip:12345678@itasp.com>
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	1

Keyword	Sub Types	Attributes
Name	String	Read/Write
Param	Param	Read/Write
URL	URL Structure (see 'URL' on page 795)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a P-Associated-Uri header to all INVITE response messages: <pre>MessageManipulations 5 = 1, register.response, ,header.P-Associated-URI, 0, '<sip:admin@10.132.10.108>', 0;</pre>
	Result:	P-Associated-URI:<sip:admin@10.132.10.108>
Example 2	Rule:	Modify the user portion of the URL in the header to 'alice': <pre>MessageManipulations 5 = 1, register.response, ,header.P-Associated-URI.url.user, 2, 'alice', 0;</pre>
	Result:	P-Associated-URI:<sip:alice@10.132.10.108>

C.2.14 P-Called-Party-Id

An example of the header is shown below:

```
P-Called-Party-ID: <sip:2000@gw.itsp.com>
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
Name	String	Read/Write
URL	URL Structure (see 'URL' on page 795)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a P-Called-Party-Id header to all messages: <pre>MessageManipulations 8 = 1, any, , header.p-called- party-id, 0, 'sip:2000@MSBG.ITSP.COM', 0;</pre>
	Result:	P-Called-Party-ID: <sip:2000@gw.itsp.com>
Example 2	Rule:	Append a parameter (p1) to all P-Called-Party-Id headers: <pre>MessageManipulations 9 = 1, invite, , header.p-called- party-id.param.p1, 0, 'red', 0;</pre>
	Result:	P-Called-Party-ID: <sip:2000@gw.itsp.com>;p1=red
Example 3	Rule:	Add a display name to the P-Called-Party-Id header: <pre>MessageManipulations 3 = 1, any, , header.p-called- party-id.name, 2, 'Secretary', 0;</pre>
	Result:	P-Called-Party-ID: Secretary <sip:2000@gw.itsp.com>;p1=red

C.2.15 P-Charging-Vector

An example of the header is shown below:

```
P-Charging-Vector: icid-value=1234bc9876e; icid-generated-at=192.0.6.8; orig-ioi=home1.net
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	No	N/A

Keyword	Sub Types	Attributes
N/A	N/A	N/A

Below are header manipulation examples:

Rule:	Add a P-Charging-Vector header to all messages: <pre>MessageManipulations 1 = 1, any, , header.P-Charging-Vector, 0, " 'icid-value=1234bc9876e; icid-generated-at=192.0.6.8; orig-ioi=home1.net' ", 0;</pre>
Result:	<pre>P-Charging-Vector: icid-value=1234bc9876e; icid-generated-at=192.0.6.8; orig-ioi=home1.net</pre>

C.2.16 P-Preferred-Identity

An example of the header is shown below:

```
P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@abc.com>
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
Name	String	Read/Write
URL	URL Structure (see 'URL' on page 795)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a P-Preferred-Identity header to all messages: <pre>MessageManipulations 1 = 1, any, , header.P-Preferred-Identity, 0, "'Cullen Jennings <sip:fluffy@abc.com>' ", 0;</pre>
	Result:	<pre>P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@abc.com></pre>
Example 2	Rule:	Modify the display name in the P-Preferred-Identity header: <pre>MessageManipulations 2 = 1, any, , header.P-Preferred-Identity.name, 2, "'Alice Biloxi'", 0;</pre>

Result:	P-Preferred-Identity: "Alice Biloxi" <sip:fluffy@abc.com>
----------------	--

C.2.17 Privacy

An example of the header is shown below:

```
Privacy: none
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	No	N/A

Keyword	Sub Types	Attributes
privacy	'Privacy Struct' on page 793	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a privacy header and set it to "session": MessageManipulations 1 = 1, any, , header.Privacy, 0, "'session'", 0;
	Result:	Privacy: session
Example 2	Rule:	Add 'user' to the list: MessageManipulations 1 = 3, , , header.privacy.privacy.user, 2, '1', 0;
	Result:	Privacy: session;user

C.2.18 Proxy-Require

An example of the header is shown below:

```
Proxy-Require: sec-agree
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
Capabilities	SIPCapabilities Struct	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Proxy-Require header to the message: <pre>MessageManipulations 1 = 1, any, , header.Proxy-Require, 0, "'sec-agree'", 0;</pre>
	Result:	Proxy-Require: sec-agree
Example 2	Rule:	Modify the Proxy-Require header to itsp.com: <pre>MessageManipulations 2 = 1, any, , header.Proxy-Require, 2, "'itsp.com' ", 0;</pre>
	Result:	Proxy-Require: itsp.com
Example 3	Rule:	Set the privacy options tag in the Proxy-Require header: <pre>MessageManipulations 0 = 0, invite, , header.Proxy-Require.privacy, 0, "1" , 0;</pre>
	Result:	Proxy-Require: itsp.com, privacy

C.2.19 Reason

An example of the header is shown below:

```
Reason: SIP ;cause=200 ;text="Call completed elsewhere"
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
MLPP	MLPP Structure (see 'MLPP' on page 793)	Read/Write
Reason	Reason Structure (see 'Reason Structure' on page 794)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Reason header: <pre>MessageManipulations 0 = 1, any, ,header.reason, 0, "'SIP;cause=200;text=\"Call completed elsewhere\"'", 0;</pre>
	Result:	Reason: SIP ;cause=200 ;text="Call completed elsewhere"
Example 2	Rule:	Modify the reason cause number: <pre>MessageManipulations 0 = 1, any, ,header.reason.reason.cause, 0, '200', 0;</pre>
	Result:	Reason: Q.850 ;cause=180 ;text="Call completed elsewhere"
Example 3	Rule:	Modify the cause number: <pre>MessageManipulations 0 = 1, any, ,header.reason.reason.reason, 0, '483', 0;</pre>

Result:	Reason: SIP ;cause=483 ;text="483 Too Many Hops"
----------------	--

Note: The protocol (SIP or Q.850) is controlled by setting the cause number to be greater than 0. If the cause is 0, then the text string (see Example 3) is generated from the reason number.

C.2.20 Referred-By

An example of the header is shown below:

```
Referred-By: <sip:referrer@referrer.example>;
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
param	param	Read/Write
URL	URL Structure (see 'URL' on page 795)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Referred-By header: <pre>MessageManipulations 0 = 1, any, ,header.Referred-By, 0, "<sip:refer@refer.com>", 0;</pre>
	Result:	Referred-By: <sip: sip:refer@refer.com>
Example 2	Rule:	Modify the host: <pre>MessageManipulations 0 = 1, any, ,header.Referred-By.url.host, 0, "'yahoo.com'", 0;</pre>
	Result:	Referred-By: <sip:refer@yahoo.com>
Example 3	Rule:	Add a new parameter to the header: <pre>MessageManipulations 0 = 1, any, ,header.Referred-By.param.pl, 0, "'fxs'", 0</pre>
	Result:	Referred-By: <sip:referrer@yahoo.com>;pl=fxs

C.2.21 Refer-To

An example of the header is shown below:

```
Refer-To: sip:conferencel@example.com
Refer-To:
<sips:a8342043f@atlanta.example.com?Replaces=12345601%40atlanta.example.com%3bfrom-tag%3d314159%3bto-tag%3d1234567>
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	No	N/A

Keyword	Sub Types	Attributes
N/A	N/A	N/A

Below are header manipulation examples:

Example 1	Rule :	Add a basic header: <pre>MessageManipulations 0 = 1, any, ,header.Refer-to, 0, "'<sip:referto@referto.com>'", 0;</pre>
	Result :	<pre>Refer-To: <sip:referto@referto.com></pre>
Example 2	Rule :	Add a Refer-To header with URI headers: <pre>MessageManipulations 0 = 1, any, ,header.Refer-to, 0, "'<sips:a8342043f@atlanta.example.com?Replaces=12345601%40atlanta.example.com%3bfrom-tag%3d314159%3bto-tag%3d1234567>'", 0;</pre>
	Result :	<pre>Refer-To: <sips:a8342043f@atlanta.example.com?Replaces=12345601%40atlanta.example.com%3bfrom-tag%3d314159%3bto-tag%3d1234567></pre>

C.2.22 Remote-Party-Id

An example of the header is shown below:

```
Remote-Party-ID: "John Smith"
<sip:john.smith@itsp.com>;party=calling; privacy=full;screen=yes
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	3

Keyword	Sub Types	Attributes
Counter	Integer	Read/Write
Name	String	Read/Write
NumberPlan	Enum Number Plan (see 'Number Plan' on page 799)	Read/Write
NumberType	Enum Number Type (see 'NumberType' on page 799)	Read/Write
Param	Param	Read/Write
Privacy	Enum Privacy (see 'Privacy' on page 800)	Read/Write
Reason	Enum Reason (RPI) (see 'Reason (Remote-Party-Id)' on page 803)	Read/Write
Screen	Enum Screen (see 'Screen' on page 803)	Read/Write
ScreenInd	Enum ScreenInd (see 'ScreenInd' on page 803)	Read/Write
URL	URL Structure (see 'URL' on page 795)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Remote-Party-Id header to the message: <pre>MessageManipulations 0 = 1, invite, ,header.REMOTE- PARTY-ID, 0, "'<sip:999@10.132.10.108>;party=calling'", 0;</pre>
	Result:	Remote-Party-ID: <pre><sip:999@10.132.10.108>;party=calling;npi=0;ton=0</pre>
Example 2	Rule:	Create a Remote-Party-Id header using the url in the From header using the + operator to concatenate strings: <pre>MessageManipulations 0 = 1, Invite, ,header.REMOTE- PARTY-ID, 0, "'<'+header.from.url +'>' + ';party=calling'", 0;</pre>
	Result:	Remote-Party-ID: <pre><sip:555@10.132.10.128;user=phone>;party=calling;npi =0;ton=0</pre>
Example 3	Rule:	Modify the number plan to 1 (ISDN): <pre>MessageManipulations 1 = 1, invite, , header.Remote- Party-ID.numberplan, 2, '1', 0;</pre>
	Result:	Remote-Party-ID: <pre><sip:555@10.132.10.128;user=phone>;party=calling;npi =1;ton=0</pre>
Example 4	Rule:	Modify the Remote-Party-Id header to set the privacy parameter to 1 (Full): <pre>MessageManipulations 1 = 1, invite, , header.Remote- Party-ID.privacy, 2, '1', 0;</pre>
	Result:	Remote-Party-ID: <pre><sip:555@10.132.10.128;user=phone>;party=calling;pri vacy=full;npi=0;ton=0</pre>

C.2.23 Request-Uri

An example of the header is shown below:

```
sip:alice:secretword@atlanta.com;transport=tcp
SIP/2.0 486 Busy Here
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	No	No	Yes	NA

Keyword	Sub Types	Attributes
Method	String	Read/Write
MethodType	Enum	Read/Write
URI	String	Read/Write
URL	URL Structure (see 'URL' on page 795)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Test the Request-URI transport type. If 1 (TCP), then modify the URL portion of the From header: <pre>MessageManipulations 1 = 1, Invite.request, "header.REQUEST-URI.url.user == '101'", header.REMOTE- PARTY-ID.url, 2, 'sip:3200@110.18.5.41;tusunami=0', 0;</pre>
	Result:	Remote-Party-ID: <sip:3200@110.18.5.41;tusunami=0>;party=calling;npi=0; ton=0
Example 2	Rule:	If the method type is 5 (INVITE), then modify the Remote-Party-Id header: <pre>MessageManipulations 2 = 1, Invite.request, "header.REQUEST-URI.methodtype == '5'", header.REMOTE- PARTY-ID.url, 2, 'sip:3200@110.18.5.41;tusunami=0', 0;</pre>
	Result:	Remote-Party-ID: <sip:3200@110.18.5.41;tusunami=0>;party=calling;npi=0; ton=0
Example 3	Rule:	For all request URI's whose method types are 488, modify the message type to a 486: <pre>MessageManipulations 1 = 1, , header.request- uri.methodtype=='488', header.request-uri.methodtype, 2, '486', 0;</pre>
	Result:	SIP/2.0 486 Busy Here

C.2.24 Require

An example of the header is shown below:

```
Require: 100rel
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
Capabilities	SIPCapabilities Struct	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Require header to all messages: <pre>MessageManipulations 1 = 1, , header.require, 0, "'early-session,em,replaces'", 0;</pre>
	Result:	Require: em,replaces,early-session
Example 2	Rule:	If a Require header exists, then delete it: <pre>MessageManipulations 2 = 1, Invite, "header.require exists" ,header.require, 1, "", 0;</pre>
	Result:	The Require header is deleted.
Example 3	Rule:	Set the early media options tag in the header: <pre>MessageManipulations 0 = 0, invite, , header.require.earlymedia, 0, "1" , 0;</pre>

	Result:	Require: em,replaces,early-session, early-media
Example 4	Rule:	Set the privacy options tag in the Require header: <pre>MessageManipulations 0 = 0, invite, , header.require.privacy, 0, "1" , 0;</pre>
	Result:	Require: em,replaces,early-session, privacy

C.2.25 Resource-Priority

An example of the header is shown below:

```
Resource-Priority: wps.3
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	2

Keyword	Sub Types	Attributes
Namespace	String	Read/Write
RPriority	String	Read/Write

C.2.26 Retry-After

An example of the header is shown below:

```
Retry-After: 18000
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
Time	Integer	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Retry-After header: <pre>MessageManipulations 2 = 1, Invite, ,header.Retry- After, 0, "'3600'", 0;</pre>
	Result:	Retry-After: 3600
Example 2	Rule:	Modify the Retry-Time in the header to 1800: <pre>MessageManipulations 3 = 1, Invite, ,header.Retry- After.time, 2, "'1800'", 0;</pre>
	Result:	Retry-After: 1800

C.2.27 Server or User-Agent

An example of the header is shown below:

```
User-Agent: Sip Message Generator V1.0.0.5
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
N/A	N/A	N/A

Below are header manipulation examples:

Example 1	Rule:	Remove the User-Agent header: <pre>MessageManipulations 2 = 1, Invite, ,header.user-agent, 1, "", 0;</pre>
	Result:	The header is removed.
Example 2	Rule:	Change the user agent name in the header: <pre>MessageManipulations 3 = 1, Invite, ,header.user-agent, 2, "itsp analogue gateway", 0;</pre>
	Result:	User-Agent: itsp analog gateway

C.2.28 Service-Route

An example of the header is shown below:

```
Service-Route: <sip:P2.HOME.EXAMPLE.COM;lr>,  
<sip:HSP.HOME.EXAMPLE.COM;lr>
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	7

Keyword	Sub Types	Attributes
ServiceRoute	String	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add two Service-Route headers: <pre>MessageManipulations 1 = 1, Invite, ,header.service-route, 0, "<P2.HOME.EXAMPLE.COM;lr>", 0; MessageManipulations 2 = 1, Invite, ,header.service-route, 0, "<sip:HSP.HOME.EXAMPLE.COM;lr>", 0;</pre>
	Result:	Service-Route:<P2.HOME.EXAMPLE.COM;lr> Service-Route: <sip:HSP.HOME.EXAMPLE.COM;lr>
Example 2	Rule:	Modify the Service-Route header in list entry 1: <pre>MessageManipulations 3 = 1, Invite, ,header.service-route.1.serviceroute, 2, "<sip:itsp.com;lr>", 0;</pre>

	Result:	Service-Route:sip:itsp.com;lr Service-Route: <sip:HSP.HOME.EXAMPLE.COM;lr>
Example 3	Rule:	Modify the Service-Route header in list entry 0: MessageManipulations 4 = 1, Invite, ,header.service-route.0.serviceroute, 2, "'<sip:home.itsp.com;lr>'", 0;
	Result:	Service-Route:sip:home.itsp.com;lr Service-Route: <sip:itsp.com;lr>

C.2.29 Session-Expires

An example of the header is shown below:

```
Session-Expires: 480
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
Param	Param	Read/Write
Refresher	Enum Refresher (see 'Refresher' on page 803)	Read/Write
Time	Integer	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add a Session-Expires header: MessageManipulations 0 = 1, any, , header.Session-Expires, 0, "'48' + '0'", 0;
	Result:	Session-Expires: 480
Example 2	Rule:	Modify the Session-Expires header to 300: MessageManipulations 1 = 1, any, , header.Session-Expires.time, 2, "'300'", 0;
	Result:	Session-Expires: 300
Example 3	Rule:	Add a param called longtimer to the header: MessageManipulations 1 = 1, any, , header.Session-Expires.param.longtimer, 0, "'5'", 0;
	Result:	Session-Expires: 480;longtimer=5
Example 4	Rule:	Set the refresher to 1 (UAC): MessageManipulations 3 = 1, any, , header.session-expires.refresher, 2, '1', 0;
	Result:	Session-Expires: 300;refresher=uac;longtimer=5

C.2.30 Subject

An example of the header is shown below:

Subject: A tornado is heading our way!

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
Subject	String	Read/Write

Below is a header manipulation example:

Rule:	Add a Subject header: <pre>MessageManipulations 0 = 1, any, , header.Subject, 0, "'A tornado is heading our way!'", 0;</pre>
Result:	Subject: A tornado is heading our way!

C.2.31 Supported

An example of the header is shown below:

Supported: early-session

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
Capabilities	SIPCapabilities Struct	Read/Write

Below is a header manipulation example:

Example 1	Rule:	Add a Supported header: <pre>MessageManipulations 1 = 1, Invite, ,header.supported, 0, "'early-session'", 0;</pre>
	Result:	Supported: early-session
Example 2	Rule:	Set path in the Supported headers options tag: <pre>MessageManipulations 0 = 0, invite, , header.supported.path, 0, "true", 0;</pre>
	Result:	Supported: early-session, path

C.2.32 To

An example of the header is shown below:

```
To: <sip:101@10.132.10.128;user=phone>
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	No	No	No	NA

Keyword	Sub Types	Attributes
Name	String	Read/Write
Param	Param	Read/Write
tag	String	Read Only
URL	URL Structure (refer to 'URL' on page 795)	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Set the user phone Boolean to be false in the To header's URL: <pre>MessageManipulations 4 = 1, invite.request, , header.to.url.UserPhone, 2, '0', 0;</pre>
	Result:	To: <sip:101@10.132.10.128>
Example 2	Rule:	Change the URL in the To header: <pre>MessageManipulations 4 = 1, invite.request, , header.to.url.UserPhone, 2, '0', 0;</pre>
	Result:	To: <sip:101@10.20.30.60:65100>
Example 3	Rule:	Set the display name to 'Bob': <pre>MessageManipulations 5 = 1, invite.request, , header.to.name, 2, "'Bob'", 0;</pre>
	Result:	To: "Bob Dylan" sip:101@10.20.30.60:65100
Example 4	Rule:	Add a proprietary parameter to all To headers: <pre>MessageManipulations 6 = 1, invite.request, , header.to.param.artist, 0, "'singer'", 0;</pre>
	Result:	To: "Bob Dylan" <sip:101@10.20.30.60:65100>;artist=singer

C.2.33 Unsupported

An example of the header is shown below:

```
Unsupported: 100rel
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	N/A

Keyword	Sub Types	Attributes
Capabilities	SIPCapabilities Struct	Read/Write

Below are header manipulation examples:

Example 1	Rule:	Add an Unsupported header to the message: <pre>MessageManipulations 0 = 1, Invite.response, ,header.unsupported, 0, "'early-session, myUnsupportedHeader'", 0;</pre>
	Result:	Unsupported: early-session
Example 2	Rule:	Modify the Unsupported header to 'replaces': <pre>MessageManipulations 1 = 1, Invite, ,header.unsupported, 2, "'replaces'", 0;</pre>
	Result:	Unsupported: replaces
Example 3	Rule:	Set the path in the Unsupported headers options tag: <pre>MessageManipulations 0 = 0, invite, , header.unsupported.path, 0, "true", 0;</pre>
	Result:	Unsupported: replaces, path

C.2.34 Via

An example of the header is shown below:

```
Via: SIP/2.0/UDP 10.132.10.128;branch=z9hG4bKUGOKMQPAVFKTAVYDQPTB
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	No	No	No	10

Keyword	Sub Types	Attributes
Alias	Boolean	Read Only
Branch	String	Read Only
Host	Host Structure (see 'Host' on page 793)	Read Only
MAddrIp	gnTIPAddress	Read Only
Param	Param	Read/Write

Keyword	Sub Types	Attributes
Port	Integer	Read Only
TransportType	Enum TransportType (see 'TransportType' on page 804)	Read Only

Below is a header manipulation example:

Rule:	Check the transport type in the first Via header and if it's set to UDP, then modify the From header's URL: <pre>MessageManipulations 0 = 1, Invite.request, "header.VIA.0.transporttype == '0'", header.from.url, 2, 'sip:3200@110.18.5.41;tusunami=0', 0;</pre>
Result:	From: <sip:3200@110.18.5.41;user=phone;tusunami=0>;tag=1c7874

C.2.35 Warning

An example of the header is shown below:

```
Warning: 307 isi.edu "Session parameter 'foo' not understood"
Warning: 301 isi.edu "Incompatible network address type 'E.164'"
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	1

Keyword	Sub Types	Attributes
N/A	N/A	N/A

Below is a header manipulation example:

Rule:	Add a Warning header to the message: <pre>MessageManipulations 0 = 1, Invite.response.180, ,header.warning, 0, "'Incompatible 380'", 0;</pre>
Result:	Warning: Incompatible 380

C.2.36 Unknown Header

An Unknown header is a SIP header that is not included in this list of supported headers. An example of the header is shown below:

```
MYEXP: scooby, doo, goo, foo
```

The header properties are shown in the table below:

Header Level Action	Add	Delete	Modify	List Entries
Operations Supported	Yes	Yes	Yes	3

Keyword	Sub Types	Attributes
N/A	N/A	N/A

Below are header manipulation examples:

Example 1	Rule:	Add a custom header to all messages: <pre>MessageManipulations 0 = 1, , , header.myExp, 0, "'scooby, doo, goo, foo'", 0;</pre>
	Result:	MYEXP: scooby, doo, goo, foo
Example 2	Rule:	Take the value from the Expires parameter in the Contact header, append 00 to the value and create a new myExp header: <pre>MessageManipulations 0 = 1, any, , header.media, 0, "header.Session-Expires.time + '000' + ';refresher=' + header.Session-Expires.Refresher", 0;</pre>
	Result:	MEDIA: 3600000;refresher=1
Example 3	Rule:	Create lists of Unknown headers: <pre>MessageManipulations 1 = 1, Invite, , header.myExp.1, 0, "'scooby, doo, goo, foo1'", 0; MessageManipulations 2 = 1, Invite, , header.myExp.2, 0, "'scooby, doo, goo, foo2'", 0;</pre>
	Result:	MYEXP: scooby, doo, goo, foo1 MYEXP: scooby, doo, goo, foo2
Example 4	Rule:	Remove the SIP header 'colour' from INVITE messages: <pre>MessageManipulations 1 = 1, Invite, , header.colour, 1, "''", 0;</pre>
	Result:	The colour header is removed.

C.3 Structure Definitions

C.3.1 Event Structure

The Event structure is used in the Event header (see 'Event' on page 773).

Table C-2: Event Structure

Keyword	Sub Types	Attributes
EventPackage	Enum Event Package (see 'Event Package' on page 798)	Read/Write
EventPackageString*	String	Read/Write
Id	String	Read/Write

Event package string is used for packages that are not listed in the Enum Event Package table (see 'Event Package' on page 798).

C.3.2 Host

The host structure is applicable to the URL structure (see 'URL' on page 795) and the Via header (see 'Via' on page 790).

Table C-3: Host Structure

Keyword	Sub Types
Port	Short
Name	String

C.3.3 MLPP

This structure is applicable to the Reason header (see 'Reason' on page 780).

Table C-4: MLPP Structure

Keyword	Sub Types
Type	Enum MLPP Reason (see 'MLPP Reason Type' on page 799)
Cause	Int

C.3.4 Privacy Struct

This structure is applicable to the Privacy header (see 'Privacy' on page 779).

Table C-5: Privacy Structure

Keyword	Sub Types
NONE	Boolean

Keyword	Sub Types
HEADER	Boolean
SESSION	Boolean
USER	Boolean
CRITICAL	Boolean
IDENTITY	Boolean
HISTORY	Boolean

C.3.5 Reason Structure

This structure is applicable to the Reason header (see 'Reason' on page 780).

Table C-6: Reason Structure

Keyword	Sub Types
Reason	Enum Reason (see 'Reason (Reason Structure)' on page 800)
Cause	Int
Text	String

C.3.6 SIPCapabilities

This structure is applicable to the following headers:

- Supported (see 'Supported' on page 788)
- Require (see 'Require' on page 784)
- Proxy-Require (see 'Proxy-Require' on page 779)
- Unsupported (see 'Unsupported' on page 790)

Table C-7: SIPCapabilities Structure

Keyword	Sub Types
EarlyMedia	Boolean
ReliableResponse	Boolean
Timer	Boolean
EarlySession	Boolean
Privacy	Boolean
Replaces	Boolean
History	Boolean
Unknown	Boolean
GRUU	Boolean
ResourcePriority	Boolean
TargetDialog	Boolean
SdpAnat	Boolean

C.3.7 URL

This structure is applicable to the following headers:

- Contact (see 'Contact' on page [771](#))
- Diversion (see 'Diversion' on page [772](#))
- From (see 'From' on page [773](#))
- P-Asserted-Identity (see 'P-Asserted-Identity' on page [776](#))
- P-Associated-Uri (see 'P-Associated-Uri' on page [776](#))
- P-Called-Party-Id (see 'P-Called-Party-Id' on page [777](#))
- P-Preferred-Identity (see 'P-Preferred-Identity' on page [778](#))
- Referred-By (see 'Referred-By' on page [781](#))
- Refer-To (see 'Refer-To' on page [781](#))
- Remote-Party-Id (see 'Remote-Party-Id' on page [782](#))
- Request-Uri (see 'Request-Uri' on page [783](#))
- To (see 'To' on page [789](#))

Table C-8: URL Structure

Keyword	Sub Types
Type	Enum Type (see 'Type' on page 804)
Host	Host Structure (see 'Host' on page 793)
MHost	Structure
UserPhone	Boolean
LooseRoute	Boolean
User	String
TransportType	Enum Transport (see 'TransportType' on page 804)
Param	Param

C.4 Random Type

Manipulation rules can include random strings and integers. An example of a manipulation rule using random values is shown below:

```
MessageManipulations 4 = 1, Invite.Request, , Header.john, 0,
rand.string.56.A.Z, 0;
```

In this example, a header called "john" is added to all INVITE messages received by the device and a random string of 56 characters containing characters A through Z is added to the header.

For a description of using random values, see the subsequent subsections.

C.4.1 Random Strings

The device can generate random strings in header manipulation rules that may be substituted where the type 'String' is required. The random string can include up to 298 characters and include a range of, for example, from a to z or 1 to 10. This string is used in the table's 'Action Value' field.

The syntax for using random strings is:

```
Rand.string.<number of characters in string>.<low character>.<high
character>
```

Examples:

- Rand.string.5.a.z: This generates a 5-character string using characters a through z.
- Rand.string.8.0.z: This generates an 8-character string using characters and digits.

C.4.2 Random Integers

The device can generate a random numeric value that may be substituted where the type 'Int' is required. The syntax for random numeric values is:

```
Rand.number.<low number>.<high number>
```

Examples:

- Rand.number.5.32: This generates an integer between 5 and 32

C.5 Wildcarding for Header Removal

The device supports the use of the "*" wildcard character to remove headers. The "*" character may only appear at the end of a string. For example, "X-*" is a valid wildcard request, but "X-*ID" is not.

Below are examples of using the wildcard:

- header.p-* - removes all headers that have the prefix "p-"
- header.via* - removes all Via headers
- header.x-vendor* - removes all headers that start with "x-vendor"
- header.* - removes all non-critical headers
- header.to* - removes all headers that start with "to", except the To header, which is protected



Note: The wildcard does not remove the following headers: Request-Uri, Via, From, To, Callid, Cseq, and Contact.

C.6 Copying Information between Messages using Variables

You can use variables in SIP message manipulation rules to copy specific information from one message to another. Information from one message is copied to a variable and then information from that variable is copied to any subsequent message. The device can store information in local or global variables. Local variables are stored on a per call basis and change when a new call is made. Up to two local variables can be used per call. Global variables do not change as new calls are made. Up to 10 global variables can be used.

The syntax for using variables is as follows:

- `Var.call.<src || dst><local index>`
where *local index* is an integer between 1 and 2 inclusive
- `Var.global.<global index>`
where *global index* is an integer between 1 and 10 inclusive

To store data in a variable, add the name of the variable in the Action Subject field and set the Action Type to Modify. To retrieve data from a variable, add it in the Action Value field and it can be used in any manipulation where a `ManStringElement` is valid as an Action Subject.

Below are example of manipulation rules implementing variables:

- Example 1:
 - Store a value in a call variable: Stores the subject URI parameter from the To header:


```
MessageManipulations 0 = 0, Invite.Request, ,
var.call.dst.1, 2, header.to.url.param.subject, 0;
```
 - Use the stored value: Allocates a Subject header for the 200 OK response for the same call and assigns it the stored value:


```
MessageManipulations 0 = 0, Invite.response.200, ,
header.subject, 0, var.call.dst.1, 0;
```
- Example 2:
 - Store a value in a global variable: Stores the Priority header of the INVITE with 'company' in the host part of the From header:


```
MessageManipulations 0 = 0, Invite.Request,
header.from.url.host == 'company', var.global.1, 2,
header.priority, 0;
```
 - Use the stored value: Assigns the same priority as the INVITE request to SUBSCRIBE requests arriving with 'company' in the host part of the From header:


```
MessageManipulations 0 = 0, Subscribe.request,
header.from.url.host == 'company', header.priority, 0,
var.global.1, 0;
```

C.7 Enum Definitions

C.7.1 AgentRole

These ENUMs are applicable to the Server or User-Agent headers (see 'Server or User-Agent' on page 786).

Table C-9: Enum Agent Role

AgentRole	Value
Client	1
Server	2

C.7.2 Event Package

These ENUMs are applicable to the Server or User-Agent (see 'Server or User-Agent' on page 786) and Event (see 'Event' on page 773) headers.

Table C-10: Enum Event Package

Package	Value
TELEPHONY	1
REFER	2
REFRESH	3
LINE_STATUS	4
MESSAGE_SUMMARY	5
RTCPXR	6
SOFT_SYNC	7
CHECK_SYNC	8
PSTN	9
DIALOG_PACKAGE	10
REGISTRATION	11
START_CWT	12
STOP_CWT	13
UA_PROFILE	14
LINE_SEIZE	15

C.7.3 MLPP Reason Type

These ENUMs are applicable to the MLPP Structure (see 'MLPP' on page 793).

Table C-11: Enum MLPP Reason Type

Type	Value
PreEmption Reason	0
MLPP Reason	1

C.7.4 Number Plan

These ENUMs are applicable to the Remote-Party-Id header (see 'Remote-Party-Id' on page 782).

Table C-12: Enum Number Plan

Plan	Value
ISDN	1
Data	3
Telex	4
National	8
Private	9
Reserved	15

C.7.5 NumberType

These ENUMs are applicable to the Remote-Party-Id header (see 'Remote-Party-Id' on page 782).

Table C-13: Enum Number Type

Number Type	Value
INTERNATIONAL LEVEL2 REGIONAL	1
NATIONAL LEVEL1 REGIONAL	2
NETWORK PISN SPECIFIC NUMBER	3
SUBSCRIBE LOCAL	4
ABBREVIATED	6
RESERVED EXTENSION	7

C.7.6 Privacy

These ENUMs are applicable to the Remote-Party-Id (see 'Remote-Party-Id' on page 782) and Diversion (see 'Diversion' on page 772) headers.

Table C-14: Enum Privacy

Privacy Role	Value
Full	1
Off	2

C.7.7 Reason (Diversion)

These ENUMs are applicable to the Diversion header (see 'Diversion' on page 772).

Table C-15: Enum Reason

Reason	Value
Busy	1
No Answer	2
Unconditional	3
Deflection	4
Unavailable	5
No Reason	6
Out of service	7

C.7.8 Reason (Reason Structure)

These ENUMs are used in the Reason Structure (see 'Reason Structure' on page 794).

Table C-16: Enum Reason (Reason Structure)

Reason	Value
INVITE	5
REINVITE	6
BYE	7
OPTIONS	8
ACK	9
CANCEL	10
REGISTER	11
INFO	12
MESSAGE	13
NOTIFY	14

Reason	Value
REFER	15
SUBSCRIBE	16
PRACK	17
UPDATE	18
PUBLISH	19
LAST_REQUEST	20
TRYING_100	100
RINGING_180	180
CALL_FORWARD_181	181
QUEUED_182	182
SESSION_PROGRESS_183	183
OK_200	200
ACCEPTED_202	202
MULTIPLE_CHOICE_300	300
MOVED_PERMANENTLY_301	301
MOVED_TEMPORARILY_302	302
SEE_OTHER_303	303
USE_PROXY_305	305
ALTERNATIVE_SERVICE_380	380
BAD_REQUEST_400	400
UNAUTHORIZED_401	401
PAYMENT_REQUIRED_402	402
FORBIDDEN_403	403
NOT_FOUND_404	404
METHOD_NOT_ALLOWED_405	405
NOT_ACCEPTABLE_406	406
AUTHENTICATION_REQUIRED_407	407
REQUEST_TIMEOUT_408	408
CONFLICT_409	409
GONE_410	410
LENGTH_REQUIRED_411	411
CONDITIONAL_REQUEST_FAILED_412	412
REQUEST_TOO_LARGE_413	413
REQUEST_URI_TOO_LONG_414	414
UNSUPPORTED_MEDIA_415	415
UNSUPPORTED_URI_SCHEME_416	416

Reason	Value
UNKNOWN_RESOURCE_PRIORITY_417	417
BAD_EXTENSION_420	420
EXTENSION_REQUIRED_421	421
SESSION_INTERVAL_TOO_SMALL_422	422
SESSION_INTERVAL_TOO_SMALL_423	423
ANONYMITY_DISALLOWED_433	433
UNAVAILABLE_480	480
TRANSACTION_NOT_EXIST_481	481
LOOP_DETECTED_482	482
TOO_MANY_HOPS_483	483
ADDRESS_INCOMPLETE_484	484
AMBIGUOUS_485	485
BUSY_486	486
REQUEST_TERMINATED_487	
NOT_ACCEPTABLE_HERE_488	488
BAD_EVENT_489	489
REQUEST_PENDING_491	491
UNDECIPHERABLE_493	493
SECURITY_AGREEMENT_NEEDED_494	494
SERVER_INTERNAL_ERROR_500	500
NOT_IMPLEMENTED_501	501
BAD_GATEWAY_502	502
SERVICE_UNAVAILABLE_503	503
SERVER_TIME_OUT_504	504
VERSION_NOT_SUPPORTED_505	505
MESSAGE_TOO_LARGE_513	513
PRECONDITION_FAILURE_580	580
BUSY_EVERYWHERE_600	600
DECLINE_603	603
DOES_NOT_EXIST_ANYWHERE_604	604
NOT_ACCEPTABLE_606	606

C.7.9 Reason (Remote-Party-Id)

These ENUMs are applicable to the Remote-Party-Id header (see 'Remote-Party-Id' on page 782).

Table C-17: Enum Reason (RPI)

Reason	Value
Busy	1
Immediate	2
No Answer	3

C.7.10 Refresher

These ENUMs are used in the Session-Expires header (see 'Session-Expires' on page 787).

Table C-18: Enum Refresher

Refresher String	Value
UAC	1
UAS	2

C.7.11 Screen

These ENUMs are applicable to the Remote-Party-Id (see 'Remote-Party-Id' on page 782) and Diversion (see 'Diversion' on page 772) headers.

Table C-19: Enum Screen

Screen	Value
Yes	1
No	2

C.7.12 ScreenInd

These ENUMs are applicable to the Remote-Party-Id header (see 'Remote-Party-Id' on page 782).

Table C-20: Enum ScreenInd

Screen	Value
User Provided	0
User Passed	1
User Failed	2
Network Provided	3

C.7.13 TransportType

These ENUMs are applicable to the URL Structure (see 'URL' on page 795) and the Via header (see 'Via' on page 790).

Table C-21: Enum TransportType

TransportType	Value
UDP	0
TCP	1
TLS	2
SCTP	3

C.7.14 Type

These ENUMs are applicable to the URL Structure (see 'URL' on page 795).

Table C-22: Enum Type

Type	Value
SIP	1
Tel	2
Fax	3
SIPS	4

C.8 Actions and Types

Element Type	Command Type	Command	Value Type	Remarks
IPGroup	Match	"=="	String	Returns true if the parameter equals to the value.
		"!="	String	Returns true if the parameter not equals to the value.
		"contains"	String	Returns true if the string given is found in the parameter value.
Call-Parameter	Match	"=="	String	Returns true if the parameter equals to the value.
		"!="	String	Returns true if the parameter not equals to the value.
		"contains"	String	Returns true if the string given is found in the parameter value.
Body	Match	"=="	String	Returns true if the body's content

Element Type	Command Type	Command	Value Type	Remarks
				equals to the value.
		"!="	String	Returns true if the body's content not equals to the value.
		"contains"	String	Returns true if the string given is found in the body's content.
		"exists"		Returns true if this body type exists in the message.
	Action	"Modify"	String	Modifies the body content to the new value.
		"Add"	String	Adds a new body to the message. If such body exists the body content is modified.
		"Remove"		Removes the body type from the message.
Header-List	Match	"=="	String *Header-list	Returns true if the header's list equals to the string.
		"!="	String *Header-list	Returns true if the header's list not equals to the string.
		"contains"	String	Returns true if the header's list contains the string.
		"exists"		Returns true if at list one header exists in the list.
	Action	"Modify"	String *Header	Removes all the headers from the list and allocates a new header with the given value.
		"Add"	String *Header	Adds a new header to the end of the list.
		"Remove"		Removes the whole list from the message.
Header	Match	"=="	String *Header	Returns true if a header equals to the value. The header element must not be a list.
		"!="	String *Header	Returns true if a header not equals to the value. The header element must not be a list.
		"contains"	String	Returns true if the header contains the string.
		"exists"		Returns true if the header exists.
	Action	"Modify"	String *Header	Replaces the entire header with the new value.

Element Type	Command Type	Command	Value Type	Remarks
		"Remove"		Removes the header from the message, if the header is part of a list only that header is removed.
		"Add"	String *Header	Adds a new header to the end of the list.
Parameter-List	Match	"=="	String Parameter-list	Returns true if the header's list equals to the string.
		"!="	String Parameter-list	Returns true if the header's list not equals to the string.
		"contains"	String	Returns true if the header's list contains the string.
		"exists"		Returns true if at list one parameter exists in the list.
	Action	"Modify"	String Parameter-list	Replaces the current parameters with the new value.
		"Add"	String Parameter	Adds a new parameter to the parameter's list.
		"Remove"		Removes all the unknown parameters from the list.
Parameter	Match	"=="	String Parameter	Returns true if the header's parameter's value equals to the value.
		"!="	String Parameter	Returns true if the header's parameter's value not equals to the value.
		"contains"	String	Returns true if the header's parameter contains the string.
		"exists"		Returns true if the header's parameter exists.
	Action	"Modify"	String Parameter	Sets the header's parameter to the value.
		"Remove"		Removes the header's parameter from the parameter list.
Structure	Match	"=="	String *Structure	Returns true if the header's structure's value equals to the value. The string given must be able to be parsed to the structure.

Element Type	Command Type	Command	Value Type	Remarks		
		"!="	String *Structure	Returns true if the header's structure's value not equals to the value. The string given must be able to be parsed to the structure.		
	Action	Modify	String *Structure	Sets the header's structure to the value. The string given must be able to be parsed to the structure.		
Integer	Match	"=="	Integer	Returns true if value equals to the integer element		
		"!="	Integer	Returns true if value not equals to the integer element		
		<td>Integer</td> <td>Returns true if value is greater than the value.</td>	Integer	Returns true if value is greater than the value.		
		<td>Integer</td> <td>Returns true if value is less than the value.</td>	Integer	Returns true if value is less than the value.		
		String	Match	"=="	String	Returns true if the string element equals to the value.
		"!="		String	Returns true if the string element not equals to the value.	
	"contains"	String		Returns true if the value is found in the string element.		
Action	"Modify"	String	Sets the string element to the value.			
	"Add prefix"	String	Adds the value to the beginning of the string element.			
	"Remove prefix"	String	Removes the value from the beginning of the string element.			
	"Add suffix"	String	Adds the value to the end of the string element.			
		"Remove suffix"	String	Removes the value from the end of the string element.		
Boolean	Match	"=="	Boolean	Returns true if the Boolean element equals to the value. Boolean – can be either "0" or "1".		

Element Type	Command Type	Command	Value Type	Remarks
		"!="	Boolean	Returns true if the Boolean element not equals to the value. Boolean – can be either "0" or "1".
	Action	"Modify"	Boolean	Sets the Boolean element to the value. Boolean – can be either "0" or "1".
Attribute	Match	"=="	Integer *Attribute	Returns true if the attribute element equals to the value. An attribute element value must be of the same type of the attribute element.
		"!="	Integer *Attribute	Returns true if the attribute element not equals to the value. An attribute element value must be of the same type of the attribute element.
	Action	Modify	Integer *Attribute	Sets the attribute element to the value. An attribute element value must be of the same type of the attribute element.

C.9 Syntax

Rules table:

Man Set ID	Message Type	Condition	Action Element	Action Type	Action Value	Row Rule
ID	<message-type>	<match-condition>	<message-element>	<action-type>	<value>	ID

1. message-type:

Description: rule is applied only if this is the message's type

Syntax: method "." message-role

Examples:

- invite.request
- invite.response.200
- subscribe.response.2xx

a. method:

Description: rule is applied only if this is the message's method

Syntax: (token / "any")

Examples:

- ◆ Invite, subscribe – rule applies only to INVITE messages
- ◆ Unknown – unknown methods are also allowed
- ◆ Any – no limitation on the method type

b. message-role

Description: rule is applied only if this is the message's role

Syntax: ("request" / "response" "." response-code / "any")

Examples:

- ◆ Request – rule applies only on requests
- ◆ Response.200 – rule applies only on 200 OK messages
- ◆ Any – no limitations on the type of the message

c. response-code

Description: response code of the message

Syntax: ("1xx" / "2xx" / "3xx" / "4xx" / "5xx" / "6xx" / 3DIGIT / "any")

Examples:

- ◆ 3xx – any redirection response
- ◆ 200 – only 200 OK response
- ◆ Any – any response

2. match-condition:

Description: matching criteria for the rule

Syntax: (message-element / param) SWS match-type [SWS value] * [SWS logical-expression SWS match-condition]

Examples:

- header.from.user == 100
- header.contact.header-param.expires > 3600
- header.to.host contains "itsp"
- param.call.dst.user != 100
- header.john exists
- header.john exists AND header.to.host !contains "john"
- header.from.user == 100 OR header.from.user == 102 OR header.from.user == 300

a. match-type

Description: comparison to be made

Syntax: ("==" / "!=" / ">" / "<" / ">=" / "<=" / "contains" / "exists" / "!exists" / "!contains")

Examples:

- ◆ "==" – equals
- ◆ "!=" – not equals
- ◆ ">" – greater than
- ◆ "<" – less than
- ◆ ">=" – greater than or equal to
- ◆ "<=" – less than or equal to
- ◆ "contains" – does a string contain a value (relevant only to string fields)
- ◆ "exists" – does a certain header exists
- ◆ "!exists" – does a certain header not exists
- ◆ "!contains" – does a string exclude a value. Relevant only to string fields

3. logical-expression:

Description: condition for the logical expression.

Syntax: ("AND" / "OR")

Examples:

- "AND" – Logical And
- "OR" – Logical Or

Note: "A AND B OR C" is calculated as A AND (B OR C).

4. message-element:

Description: element in the message

Syntax: ("header" / "body") "." message-element-name ["." header-index] * ["." (sub-element / sub-element-param)]

Examples:

- Header.from
- Header.via.2.host
- Header.contact.header-param.expires
- Header.to.uri-param.user-param
- Body.application/dtmf-relay

a. message-element-name

Description: name of the message's element - "/" only used for body types

Syntax: 1 * (token / "/")

Examples:

- ◆ from (header's name)
- ◆ to (header's name)
- ◆ application/dtmf-relay (body's name)

b. header-index

Description: header's index in the list of headers

Syntax: integer

Examples: If five Via headers arrive:

- ◆ 0 (default) – refers to the first Via header in the message
- ◆ 1 – the second Via header
- ◆ 4 – the fifth Via header

c. sub-element

Description: header's element

Syntax: sub-element-name

Examples:

- ◆ user
- ◆ host

d. sub-element-param

Description: header's element

Syntax: sub-element-name ["." sub-element-param-name]

Examples:

- ◆ header.from.param.expires

e. sub-element-param-name

Description: header's parameter name - relevant only to parameter sub-elements

Syntax: token

Examples:

- ◆ expires (contact's header's param)
- ◆ duration (retry-after header's param)
- ◆ unknown-param (any unknown param can be added/removed from the header)

f. param

Description: Params can be as values for match and action

Syntax: "param" "." Param-sub-element "." Param-dir-element "." (Call-Param-entity / ipg-param-entity)

Examples:

- ◆ param.ipg.src.user
- ◆ param.ipg.dst.host
- ◆ param.ipg.src.type
- ◆ param.call.src.user

g. param-sub-element

Description: determines whether the param being accessed is a call or an IP Group

Syntax: ("call" / "IPG")

Examples:

- ◆ call – relates to source or destination URI for the call
- ◆ ipg – relates to the source or destination IP Group

h. param-dir-element

Description: direction relating to the classification

Syntax: ("src" / "dst")

Examples:

- ◆ src – relates to the source
- ◆ dst – relates to the destination

i. call-param-entity

Description: parameters that can be accessed on the call

Syntax: ("user")

Examples:

- ◆ user – refers to the username in the request-URI for call

j. ipg-param-entity

Description: name of the parameter

Syntax: ("user" / "host" / "type" / "id")

Examples:

- ◆ user – refers to the contact user in the IP Group
- ◆ host – refers to the group name in the IP Group table
- ◆ type – refers to the type field in the IP Group table
- ◆ id - refers to the IP Group ID (used to identify source or destination IP Group)

k. string

Description: string enclosed in double quotes

Syntax: quoted-string

Examples:

- ◆ "username"
- ◆ "123"
- ◆ "user@host"

l. integer

Description: a number

Syntax: 1 * DIGIT

Example:

- ◆ 123

5. action-type:

Description: action to be performed on the element

Syntax: ("modify" / "add-prefix" / "remove-prefix" / "add-suffix" / "remove-suffix" / "add" / "remove")

Examples:

- "modify" – sets the element to the new value (all element types)
- "add-prefix" – adds the value at the beginning of the string (string element only)
- "remove-prefix" – removes the value from the beginning of the string (string element only)
- "add-suffix" – adds the value at the end of the string (string element only)
- "remove-suffix" – removes the value from the end of the string (string element only)
- "add" – adds a new header/param/body (header or parameter elements)
- "remove" – removes a header/param/body (header or parameter elements)

6. value:

Description: value for action and match

Syntax: (string / message-element / param) * ("+" (string / message-element / param))

Examples:

- "itsp.com"
- Header.from.user
- Param.ipg.src.user
- Param.ipg.dst.host + ".com"
- Param.call.src.user + "<" + header.from.user + "@" + header.p-asserted-id.host + ">"

Reader's Notes

D DSP Templates

This section lists the DSP templates supported by the device. Each DSP template provides support for specific voice coders (as well as channel capacity and various features). You can use the following parameters to select the required DSP template:

- DSP Version Template Number (DSPVersionTemplateName) - allows you to select a specific DSP template.
- DSP Templates table (DSPTemplates) - allows you to select two DSP templates for the device to use and determine the percentage of DSP resources allocated per DSP template.



Notes:

- Installation and use of voice coders is subject to obtaining the appropriate license and royalty payments.
- The number of channels refers to the maximum channel capacity of the device.
- The maximum number of channels on any form of analog, digital and MPM modules assembly is 120.
- For additional DSP templates, contact your AudioCodes representative.

D.1 Analog Interfaces

The DSP templates for analog interfaces are shown in the table below.

Table D-1: DSP Firmware Templates for Analog (FXS/FXO) Interfaces

	DSP Template	
	0, 1, 2, 4, 5, 6	10, 11, 12, 14,15, 16
	Number of Channels	
Default Settings	4	3
With SRTP	3	3
	Voice Coder	
G.711 A/Mu-law PCM	Yes	Yes
G.726 ADPCM	Yes	Yes
G.723.1	Yes	Yes
G.729 A, B	Yes	Yes
G.722	-	Yes

D.2 Digital Interfaces

The DSP templates for digital interfaces are shown in the table below.

Table D-2: DSP Firmware Templates for Digital Interfaces

	DSP Template														
	0 or 10			1 or 11			2 or 12			5 or 15			6 or 16		
	Number of Spans														
	1	2	4	1	2	4	1	2	4	1	2	4	1	2	4
	Number of Channels														
Default settings	31	62	120	31	48	80	24	36	60	24	36	60	31	60	100
With 128 ms EC	31	60	100	31	48	80	24	36	60	24	36	60	31	60	100
With SRTP	31	60	100	NA	NA	NA	24	36	60	24	36	60	31	48	80
With IPM Features (*)	31	60	100	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	31	60
With IPM Features & SRTP	31	48	80	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	31	48
Voice Coder															
G.711 A-law/Mm-law PCM	Yes			Yes			Yes			Yes			Yes		
G.726 ADPCM	Yes			Yes			Yes			Yes			-		
G.723.1	Yes			-			-			-			-		
G.729 A, B	Yes			Yes			Yes			Yes			Yes		
GSM FR	Yes			Yes			-			-			-		
MS GSM	Yes			Yes			-			-			-		
iLBC	-			-			-			Yes			-		
EVRC	-			-			Yes			-			-		
QCELP	-			-			Yes			-			-		
AMR	-			Yes			-			-			-		
GSM EFR	-			Yes			-			-			-		
G.722	-			-			-			-			Yes		
Transparent	Yes			Yes			Yes			Yes			Yes		



Notes: IPM Features refers to the configuration that includes at least one of the following:

- Mounted MPM module in Slot #6 for conference applications.
- IPM detectors (e.g., Answer Detector) are enabled.
- The IP Media Channels featured is enabled.

D.3 Media Processing Interfaces

The DSP templates for the media processing interfaces (i.e., MPM module) are shown in the table below.

**Notes:**

- The MPM module DSP templates are applicable only to Mediant 1000.
- Assembly of the MPM module in Slot #6 enables DSP conferencing capabilities.
- To use the MPM module, the device must be installed with the IP Media Channels Feature Key.

Table D-3: DSP Firmware Templates for MPM Module

Supplementary Capabilities			DSP Template									
			0 or 10		1 or 11		2 or 12		5 or 15		6 or 16	
			Assembly Slot no.									
			1-5	6	1-5	6	1-5	6	1-5	6	1-5	6
S RTP	IPM Detectors	Conference	Number of Channels									
			-	-	-	40	20	32	16	24	12	24
Yes	-	-	40	20	NA	NA	24	12	24	12	40	20
-	Yes	-	40	20	NA	NA	NA	NA	NA	NA	40	20
Yes	Yes	-	32	16	NA	NA	NA	NA	NA	NA	32	16
-	-	Yes	40	20	32	16	24	12	24	12	40	20
Yes	-	Yes	32	16	NA	NA	24	12	24	12	32	16
Yes	Yes	Yes	32	16	NA	NA	NA	NA	NA	NA	32	16
Voice Coder												
G.711 A-law/Mm-law PCM			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
G.726 ADPCM			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	-	-
G.723.1			Yes	-	-	-	-	-	-	-	-	-
G.729 A, B			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
GSM FR			Yes	Yes	-	-	-	-	-	-	-	-
MS GSM			Yes	Yes	-	-	-	-	-	-	-	-
iLBC			-	-	-	-	-	Yes	-	-	-	-
EVRC			-	-	-	Yes	-	-	-	-	-	-
QCELP			-	-	-	Yes	-	-	-	-	-	-
AMR			-	Yes	-	-	-	-	-	-	-	-
GSM EFR			-	Yes	-	-	-	-	-	-	-	-
G.722			-	-	-	-	-	-	-	-	Yes	Yes
Transparent			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

E Selected Technical Specifications

E.1 Mediant 600

The table below lists the main technical specifications of the Mediant 600.

Table E-1: Mediant 600 Functional Specifications

Function	Specification
Interfaces	
E1/T1/J1	1, 2 or fractional (15 DS0) span spans using RJ-48c connectors
BRI S/T	4 or 8 ports (8/16 calls) using RJ-45 connectors
Analog	4 FXS ports using RJ-11 connectors
Ethernet	Dual Redundant Ethernet 10/100Base-TX Ethernet ports via 2 RJ-45 connectors
RS-232	RS-232 for configuration and troubleshooting
Media Processing	
Voice Coders	G.711, G.722, G.723.1, G.729A/B, G.726, GSM FR, MS GSM, iLBC, EVRC, QCELP, AMR, GSM EFR. Independent dynamic vocoder selection per channel, VAD, CNG.
Echo Cancellation	G.165 and G.168-2002, with 32, 64 or 128 tail length.
QoS	802.1p/Q VLAN tagging, DiffServ, voice quality monitoring, RTCP-XR DTMF/MF Transport Packet side or PSTN side detection and generation, RFC 2833 compliant DTMF relay, Call Progress tone detection and generation IP Transport, VoIP (RTP/RTCP) per IETF RFC 3550 and 3551.
Fax and Modem Transport	T.38 compliant (real time fax), Automatic bypass to PCM or ADPCM.
Signaling	
E1/T1 CAS	E&M, Loop Start, Feature Group-D, E911CAMA, R2 MFC, numerous protocol and country variants
ISDN PRI	ETSI/EURO, ANSI NI2, DMS-100, 5ESS, VN3, VN4, VN6 QSIG (Basic Call and Supplementary Services) and other variants
Control & Management	
Control Protocols	SIP
Operations & Management	AudioCodes Element Management System Embedded HTTP Web Server Telnet SNMP V2/V3
Remote configuration and software download	TFTP, HTTP, HTTPS, DHCP and BootP, RADIUS, Syslog (for events, alarms and CDRs)

Function	Specification
Security	
Security Protocols	IPSec, HTTPS, TLS (SIPS), SSL, Web access list, RADIUS login and SRTP
Hardware Specifications	
Power Supply	Single universal power supply 100-240V 0.5A 50-60 Hz
Physical	1U high, 19-inch wide
Dimensions	306 x 273 x 44 mm
Regulatory Compliance	
Telecommunication Standards	TIA/EIA-IS-968, TBR-4, TBR-13, and TBR-21
Safety and EMC Standards	UL60950-1; FCC 47 CFR part 15 Class B CE Mark (EN55022: 2006, EN55024: 1998 + A1: 2001 +A2: 2003 EN6600-3-2: 2000 + A2: 2005, EN6600-3-3: 1995 + A1: 2001 EN60950-1:2001, A11: 2004)
Environmental Specifications	ETS 300019-2-1 Storage T1.2

E.2 Mediant 1000

The table below lists the main technical specifications of the Mediant 1000.

Table E-2: Mediant 1000 Functional Specifications

Function	Specification
Interfaces	
Modularity and Capacity	Voice interface: Equipped with 6 Slots that can host voice modules. Up to a maximum of 24 analog ports or 4 digital spans.
Digital Modules	1, 2 or 4 E1/T1/J1 spans using RJ-48c connectors per module. Up to 4 digital modules (maximum 4 spans per gateway). Optional 1+1 or 2+2 fallback spans.
Analog FXO and FXS Modules	4 ports using RJ-11 connectors per module; Up to 6 modules per gateway, Ground Start and Loop Start.
BRI Module	4 BRI ports (8 calls) per module, up to 5 modules per gateway with S/T interfaces. Supports Euro ISDN, NI2, 5ESS or QSIG.
Media Processing Module	Hosting media processing features: conferencing, play/record over HTTP or NFS.
I/O	MOH (Music On Hold), NB (Night Bell).
Ethernet	Dual Redundant 10/100Base-TX Ethernet ports via 2 RJ-45 connectors.
RS-232	Debugging and configuration.

Function	Specification
Media Processing	
Voice Coders	G.711, G.722, G.723.1, G.729A/B, G.726, GSM FR, MS GSM, iLBC, EVRC, QCELP, AMR, GSM EFR. Independent dynamic vocoder selection per channel.
Echo Cancellation	G.165 and G.168-2002, with 32, 64 or 128 tail length.
Quality Enhancement	Dynamic programmable jitter buffer, VAD, CNG, 802.1p/Q VLAN tagging, DiffServ, voice quality monitoring, G.729B, RTCPXR.
DTMF/MF Transport	Packet side or PSTN side detection and generation, RFC 2833 compliant DTMF relay. Call Progress tones detection and generation.
IP Transport	VoIP (RTP/RTCP) per IETF RFC 3550 and 3551.
Fax and Modem Transport	T.38 compliant (real time fax), Automatic bypass to PCM or ADPCM.
OSN Server Platform - Embedded, Partner application platform for third-party services	
CPU	<ul style="list-style-type: none"> ▪ OSN1: Intel™ Celeron™ 600 Mhz ▪ OSN2: Intel Pentium M 1.4 GHz
Memory	<ul style="list-style-type: none"> ▪ OSN1: One SODIMM slot 512M or 1G RAM ▪ OSN2: 1 or 2 GRAM
Storage	<ul style="list-style-type: none"> ▪ OSN1: Single/Dual hard disk drives ▪ OSN2: Single SATA HDD
Interfaces	<ul style="list-style-type: none"> ▪ OSN1: 10/100Base-TX, USB, RS-232, NB relay, MOH ▪ OSN2: 10/100Base-TX, USB, RS-232
Signaling	
Digital – PSTN Protocols	CAS: MF-R1: T1 CAS (E&M, Loop start, Feature Group-D, E911CAMA), E1 CAS (R2 MFC) ISDN PRI: ETSI/EURO ISDN, ANSI NI2 and other variants (DMS-100, 5ESS) QSIG (Basic and supplementary), VN3, VN4, VN6
Analog Signaling	FXS; Caller ID; polarity reversal; metering tones, distinctive ringing, visual message waiting indication, Loop Start, Ground Start
Control & Management	
Control Protocols	SIP, MSCML
Operations & Management	AudioCodes Element Management System Embedded HTTP Web Server Telnet SNMP V2, V3 Remote configuration and software download via TFTP, HTTP, HTTPS, DHCP and BootP, RADIUS, Syslog (for events, alarms and CDRs) Auto Update

Function	Specification
Security	
	IPSec, HTTPS, TLS (SIPS), SSL, Web access list, RADIUS login and SRTP2
Hardware Specifications	
Power Supply	Single universal power supply 100-240V 50-60 Hz 1.5A max., optional redundant power supply
Physical	1U high, 19-inch wide
Regulatory Compliance	
Telecommunication Standards	TIA/EIA-IS-968, TBR-4, TBR-13, and TBR-21
Safety and EMC Standards	UL60950-1; FCC 47 CFR part 15 Class B CE Mark (EN55022 Class B, EN60950-1, EN55024, EN300 386, EN61000-3-2/3-3)
Environmental Specifications	ETS 300019-2-1 Storage T1.2, ETS 300019-2-2 Transportation T2.3 ETS 300019-2-3 Operating T3.2

Reader's Notes



User's Manual Ver. 6.4